

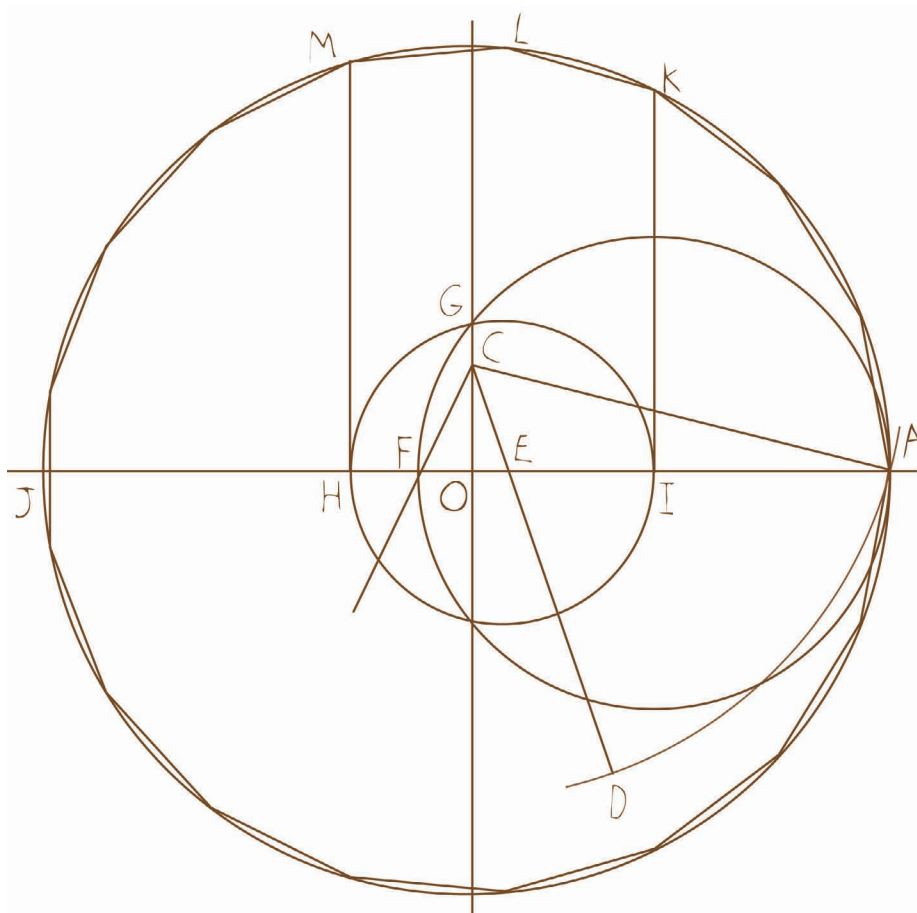
Cyclotomic Fields

with
applications



G Eric Moorhouse

CYCLOTOMIC FIELDS WITH APPLICATIONS



Lecture Notes for Math 5590
Fall 2018

G. Eric Moorhouse
University of Wyoming
©2018

Preface

These notes were written during the summer of 2018, while planning a graduate course for the Fall 2018 semester. The theme was chosen to appeal to students of varying backgrounds, some with interest primarily in number theory, and others more interested in combinatorics, graph theory and finite geometry. As it happens, my research has led me into areas of overlap between these two areas, with cyclotomic fields arising as a common theme. And so beyond the immediate goal of appealing to students with multiple interests, this course was conceived also as a way of crystallizing in my mind some of the finer points of the theory of cyclotomic fields, many of which I had less familiarity with. Students were referred primarily to Washington's book [Wa] for further details on cyclotomic fields, and various other sources as needed.

The realities of my teaching environment (perhaps yours too?) mean that I now apportion less lecture time on theory and proofs, with more on examples and applications, than when I first began teaching. In the grand tradition of mathematics, these applications arise largely in ... (wait for it!) ... other areas of mathematics. (That may not be strictly true; but as usual, our description of these applications has been rather simplified, sometimes oversimplified, to their mathematical essence, for the sake of brevity.) These applications include

- ◇ algorithms for fast arithmetic with polynomials and integers;
- ◇ constructions and nonexistence results for Hadamard matrices, difference sets, and designs, particularly nets finite affine and projective planes;
- ◇ spectra of Cayley graphs and digraphs over abelian groups;
- ◇ counting solutions to equations over finite fields;
- ◇ the MacWilliams relations for error-correcting codes;
- ◇ Dirichlet's theorem on primes on arithmetic progressions; and
- ◇ mutually unbiased bases (quantum information theory).

Given the demands of this pedagogical emphasis, there has been no single reference available where all of these developments can be found.

Another design constraint on these notes has been the varying backgrounds of our students, some will have had advanced courses in field theory or number theory, and others not. In order to keep these notes as self-contained as possible, I have included appendices containing many of the results needed from field theory and number theory, omitting the longer proofs; also omitting major results in the theory which do not bear directly upon our particular development or featured applications. I expect that during this fall semester, I will actually summarize much of the content in these appendices during the lectures, rather than leaving students to read these solely on their own.

I am indebted to many sources from which I have borrowed extensively, particularly [IR], [LN], [Sa] and [Wa]. Often this has meant rewriting content in my own way, and

adding details which other authors have left as exercises. I have also looked for ways to avoid explicitly developing all the tools required in some of the standard proofs—not that I feel these tools are unimportant for students to learn, but due to concern that the proliferation of technical definitions and warmup lemmas would overly distract students from the main points. One of my goals, in particular, is a presentation of Gluck’s Theorem 14.2 (a beautiful and very accessible argument using cyclotomic integers in a nontrivial and surprising way). Its proof, however, invokes a theorem of Segre usually formulated in the language of projective plane geometry. Not wanting to spend the extra time on such an extended detour for the majority of our students without this conceptual background, I strove instead for an alternative presentation of Segre’s Theorem in the language of affine plane geometry. I am very happy with the resulting Theorem 3.14, which I feel is also better adapted to the proof of Gluck’s Theorem than the original.

I regret omitting several major topics which a more comprehensive textbook would have included: Stickelberger’s Theorem, higher reciprocity laws, applications to algebraic coding theory and cryptology, and Bernhard Schmidt’s definitive work on the circulant Hadamard conjecture. However, in the spirit of a set of working lecture notes, my priority has been to limit the scope to only what I believe can be accomplished in a single semester. But perhaps in a future revision. . .

Throughout all my rewriting of standard material, I will certainly have added many of my own errors, for which I take full responsibility. A list of errata will be posted at

<http://ericmoorhouse.org/courses/5590/>

With each mistake/misprint that you encounter in this manuscript, please first check the website to see if it has already been listed; if not, please email me at moorhous@uwyo.edu with the necessary correction to add to this list. Thank you!

Eric Moorhouse
August, 2018

Notational Conventions

Throughout these notes, I compose functions right-to-left, as in $(\sigma\tau)(a) = \sigma(\tau(a))$. Groups are multiplicative unless otherwise indicated. The symbol ζ denotes a complex root of unity, except when it represents a zeta function (à la Riemann, Dedekind, Hasse, etc.). Likewise, ‘ i ’ signifies either an integer index (sometimes a dummy index of summation), or $\sqrt{-1}$, again depending on the context. So deal with it.

Contents

<i>Preface</i>	iii
1. Finite Cyclic Groups	1
2. Cyclotomic Polynomials	4
3. Finite Fields	8
Squares and Nonsquares	9
Automorphisms of Finite Fields	12
Polynomials versus Functions	13
Counting Irreducible Polynomials	15
Segre's Theorem	16
4. Cyclotomic Fields and Integers	19
5. Fermat's Last Theorem	29
6. Characters of Finite Abelian Groups	35
Spectra of Cayley Graphs and Digraphs	40
Error-Correcting Codes	41
The Fast Fourier Transform	44
Fast Polynomial Multiplication	46
Fast Integer Multiplication	47
7. Group Rings $R[G]$	49
The Rational Group Algebra of a Finite Cyclic Group	50
Direct Products	52
8. Difference Sets	54
9. Hadamard Matrices	64
Skew-Type Hadamard Matrices	66
Williamson-Hadamard Matrices	67
Regular Hadamard Matrices	73
Circulant Hadamard Matrices	74
10. Quadratic Reciprocity	76
11. Gauss and Jacobi Sums	84
12. Zeta Functions and L -Functions	91
13. Exponential Sums	96
14. Affine Planes	104
15. Nets	107
16. Mutually Unbiased Bases	116
17. Weil's Bound	124

Appendices

A1. Fields and Extensions	129
Matrix Representations of Field Extensions	132
A2. Polynomials and Irreducibility	136
A3. Algebraic Integers	138

A4. Normal and Separable Extensions	148
A5. Field Automorphisms and Galois Theory	153
A6. Dedekind Zeta Functions and Dirichlet Series ...	163
A7. Symmetric Polynomials	167
A8. Computational Software	170
PARI/GP	171
Mathematica	172
 <i>Bibliography</i>	 175
 <i>Index</i>	 179

1. Finite Cyclic Groups

A **cyclic group** is a group generated by a single element. A cyclic group may be finite or infinite. Every infinite cyclic group is isomorphic to the additive group of \mathbb{Z} ; or equivalently, the multiplicative subgroup $\langle \pi \rangle = \{\pi^k : k \in \mathbb{Z}\} \subset \mathbb{C}^\times$. (Here \mathbb{C}^\times is the multiplicative group of nonzero complex numbers; and one can replace π by any nonzero complex number which is not a root of unity.) Every finite cyclic group of order n is isomorphic to the additive group $\mathbb{Z}/n\mathbb{Z}$ of integers mod n ; equivalently, the multiplicative subgroup of complex n th roots of unity. The latter group is

$$\{z \in \mathbb{C} : z^n = 1\} = \langle \zeta \rangle = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$$

where $\zeta = \zeta_n$ is a **primitive n -th root of unity**, i.e. an element of order n in \mathbb{C}^\times . Recall that \mathbb{C} contains exactly $\phi(n)$ primitive n -th roots of unity $e^{2\pi ki/n}$ where $1 \leq k \leq n$, $\gcd(k, n) = 1$ and Euler's **totient function** $\phi(n)$ denotes the number of values of k satisfying the latter conditions. Evidently $\phi(n)$ is the number of generators in an arbitrary cyclic group of order n . In the preceding context, we have used the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$ in which the generators are the elements relatively prime to n .

But we will often prefer that our groups be written multiplicatively. Thus in the generic case, an arbitrary cyclic group of order $n \geq 1$ may be expressed (up to isomorphism) as a multiplicative group $G = \langle x : x^n = 1 \rangle = \{1, x, x^2, \dots, x^{n-1}\}$ generated by an element x of order n .

Theorem 1.1. Let $G = \langle x \rangle$ be a (multiplicative) cyclic group of order $n \geq 1$. Then G has $\phi(n)$ generators x^k , $1 \leq k \leq n$, $\gcd(k, n) = 1$. Every subgroup of G is cyclic of order d dividing n . Conversely, for every positive $d \mid n$, G has a unique subgroup of order d given by $\langle x^{n/d} \rangle$. Thus

$$n = \sum_{1 \leq d \mid n} \phi(d).$$

Proof. Most of Theorem 1.1 is proved by the Division Algorithm. For example if H is a subgroup of G , let $d \in \{1, 2, \dots, n\}$ be minimal such that $x^d \in H$. (Note that the set of $d \in \{1, 2, \dots, n\}$ satisfying $x^d \in H$ is nonempty since $x^n = 1 \in H$; so the minimum such d is defined.) So $\langle x^d \rangle \subseteq H$. We have $n = qd + r$ for some integers q, r with $0 \leq r < d$. If $0 < r < d$ then $x^r = x^n(x^d)^{-q} \in H$, contradicting the minimality of d ; so we must have $d \mid n$. Now $\langle x^d \rangle \subseteq H$; and to prove equality, let $h \in H$, so $h = x^j$ for some j . Again by the Division Algorithm, $j = q'd + r'$ where $0 \leq r' < d$; and again using the minimality of d , we have $r' = 0$, so $x^j = (x^d)^{q'} \in \langle x^d \rangle$. This gives $H = \langle x^d \rangle$. The relation $n = \sum_{d \mid n} \phi(d)$ follows by counting in two different ways the number of pairs (g, H) where $g \in G$ and $H = \langle g \rangle \leq G$. \square

Theorem 1.2. If G is a cyclic group of order n , then its automorphism group $\text{Aut } G$ is abelian of order $\phi(n)$. In fact, $\text{Aut } G \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of units of the ring of integers mod n .

Proof. Let $G = \{1, g, g^2, \dots, g^{n-1}\}$. For each $k \in \{1, 2, \dots, n\}$ with $\gcd(k, n) = 1$, define $\sigma_k : G \rightarrow G$ by $\sigma_k(x) = x^k$. One easily checks that σ_k is well-defined, bijective, and $\sigma_k(xy) = (xy)^k = x^k y^k = \sigma_k(x)\sigma_k(y)$. Thus $\sigma_k \in \text{Aut } G$.

Conversely, let $\sigma \in \text{Aut } G$. Since g has order n , so does $\sigma(g)$; thus $\sigma(g) = g^k$ for some $k \in \{1, 2, \dots, n\}$ with $\gcd(k, n) = 1$. It follows readily that $\sigma = \sigma_k$. (Every $x \in G$ has the form $x = g^r$ for some g ; and then $\sigma(x) = \sigma(g^r) = \sigma(g)^r = (g^k)^r = \sigma_k(g^r) = \sigma_k(x)$.) Thus $\text{Aut } G = \{\sigma_k : 1 \leq k \leq n, \gcd(k, n) = 1\}$. The map $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut } G, k \mapsto \sigma_k$ is in fact an automorphism: it is bijective, and for all $x \in G$, $(\sigma_k(\sigma_\ell(x))) = (x^\ell)^k = x^{k\ell} = \sigma_{k\ell}(x)$, so $\sigma_k\sigma_\ell = \sigma_{k\ell}$. In particular, $\text{Aut } G$ is abelian of order $\phi(n)$. \square

Caution: Do not confuse G with its automorphism group $\text{Aut } G$. Keep in mind that G and $\text{Aut } G$ do not have the same order. Theorem 1.2 *does not* say that $\text{Aut } G$ is cyclic; nor does it say that the automorphism group of an abelian group is abelian. See Exercise #4.

A function f defined on positive integers is **multiplicative** if $f(mn) = f(m)f(n)$ whenever m, n are relatively prime positive integers. (Note the condition that $\gcd(m, n) = 1$.) A function f is **completely multiplicative** if $f(mn) = f(m)f(n)$ for all m, n . We shall have reason to consider functions with this stronger property; but ϕ is not an example.)

Theorem 1.3. ϕ is multiplicative, and $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ where the product extends over all prime divisors $p|n$.

Proof. Suppose $n = ab$ where a and b are relatively prime positive integers. The natural homomorphism $f : \mathbb{Z} \rightarrow (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z})$ mapping $k \mapsto (k+a\mathbb{Z}, k+b\mathbb{Z})$ has kernel $n\mathbb{Z}$ (since this is the set of all integers divisible by both a and b). Since f is surjective, it induces a ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z}).$$

Now it is easy to see that if R_1 and R_2 are rings with identity, then the units of $R_1 \oplus R_2$ are exactly the elements (u_1, u_2) with u_i a unit in R_i . Thus

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

Taking the cardinality of both sides gives $\phi(n) = \phi(a)\phi(b)$.

If p is prime and $r \geq 1$, then the integers $k \in \{1, 2, \dots, p^r\}$ *not* relatively prime to p^r are the integers $k = p\ell$, $\ell \in \{1, 2, \dots, p^{r-1}\}$; so $\phi(p^r) = p^r - p^{r-1} = p^r(1 - \frac{1}{p})$. So the indicated formula for $\phi(n)$ holds for prime powers $n = p^r$. More generally, let n be a

positive integer and consider its prime factorization $n = \prod_{i=1}^r p_i^{e_i}$ where p_1, p_2, \dots, p_r are the distinct prime factors of n , and $e_i \geq 1$. Using multiplicativity of ϕ ,

$$\phi(n) = \prod_{i=1}^r \left[p_i^{e_i} \left(1 - \frac{1}{p_i} \right) \right] = n \prod_{i=1}^r \left(1 - \frac{1}{p_i} \right). \quad \square$$

Some textbooks use the Chinese Remainder Theorem in place of the ring isomorphism $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/a\mathbb{Z}) \oplus (\mathbb{Z}/b\mathbb{Z})$ in proving the multiplicativity of ϕ . In our view, however, it is the ring isomorphism which most naturally gives rise to *both* the Chinese Remainder Theorem and the group isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. This is a classic instance where just a modicum of abstract algebra provides a clean and insightful proof, where the alternative is a rather tedious and technical argument.

A positive integer n is **squarefree** if n is not divisible by any square integer larger than 1; equivalently, n is a product of *distinct* primes (possibly an empty product, so that 1 is squarefree). For every positive integer n , define

$$\mu(n) = \begin{cases} (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct primes;} \\ 0, & \text{if } n \text{ is not squarefree.} \end{cases}$$

Like ϕ , the function μ is multiplicative. Indeed, μ is the unique multiplicative function satisfying

$$\mu(p^k) = \begin{cases} 1, & \text{if } k = 0; \\ -1, & \text{if } k = 1; \\ 0, & \text{if } k \geq 2 \end{cases}$$

where p is prime. From Theorems 1.1 and 1.3 we obtain

$$\textbf{Theorem 1.4.} \quad \phi(n) = \sum_{1 \leq d|n} \mu\left(\frac{n}{d}\right) d = \sum_{1 \leq d|n} \frac{\mu(d)}{d} n. \quad \square$$

Note that the two formulas given are equivalent via the substitution $d \leftrightarrow \frac{n}{d}$ for divisors $d|n$. The formulas can be proved in several ways: (i) directly by mathematical induction on n , using $n = \sum_{1 \leq d|n} \phi(d)$; or (ii) using the inclusion-exclusion principle for counting the cardinalities of the subgroups $H \leq G$ where $|G|/|H|$ is squarefree; or (iii) using Möbius inversion; or (iv) by expanding the formula $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p} \right)$ from Theorem 1.3.

Exercises 1.

1. (a) Let G be a cyclic group of order n . Note that if one chooses $g \in G$ uniformly at random, the probability that $\langle g \rangle = G$ is $\frac{\phi(n)}{n} \in [0, 1]$. Show that $\limsup_{n \rightarrow \infty} \frac{\phi(n)}{n} = 1$ and $\liminf_{n \rightarrow \infty} \frac{\phi(n)}{n} = 0$. This says that in particular, the ratio $\frac{n}{\phi(n)}$ has no upper bound.
- (b) Determine the ‘limiting average value’ of $\frac{\phi(n)}{n}$, i.e. evaluate $\lim_{n \rightarrow \infty} \frac{1}{n} \left[\frac{\phi(1)}{1} + \frac{\phi(2)}{2} + \dots + \frac{\phi(n)}{n} \right]$. Some numerical data might provide an initial insight here.
2. Factorization of most integers having more than a couple hundred decimal digits, is prohibitively difficult. (In fact, no polynomial-time algorithm for integer factorization is known.) Show that computation of $\phi(n)$ for large integers is also prohibitively difficult in general. *Hint:* Consider

numbers of the form $n = pq$ where $p \neq q$ are large primes. For such numbers we have $\phi(n) = (p-1)(q-1)$. Show that any algorithm to compute $\phi(n)$ (given only the decimal representation of n) can also be used to provide the prime factorization of n .

3. To compute $\gcd(m, n)$ for small integers, one typically relies on first determining the prime factorizations of m and n . By remarks above, this approach fails for large integers. However, computation of $\gcd(m, n)$ for large integers (having several hundred digits) is very efficient using Euclid's algorithm (which runs in polynomial time). But by #2, one cannot expect to be able to compute $\phi(n)$ exactly for most large values of n .

Given a large positive integer n , one might try to *estimate* $\phi(n)$ by random sampling: Repeatedly choose k between 1 and n (uniformly distributed, using a pseudorandom number generator). After N trials, if d is the number of values of k found for which $\gcd(k, n) = 1$, we obtain an estimate $\phi(n) \approx \frac{dn}{N}$. How practical is this approach as a means to estimate $\phi(n)$? In particular can one realistically hope to approximate $\phi(n)$ to within, say, 10% of its true value? Can you suggest obvious improvements to this approach? Consider in particular (by #1) that for large values of n , there are values of n where randomly sampling $k \in \{1, 2, \dots, n\}$ *almost always* finds $\gcd(k, n) = 1$; and other values of n where random sampling *almost always* finds $\gcd(k, n) > 1$.

4. (a) Find the smallest n such that the automorphism group of a cyclic group G of order n is not cyclic. Determine the isomorphism type of G in this case.
- (b) Find the smallest abelian group G for which $\text{Aut } G$ is nonabelian. Indicate the isomorphism types of G and $\text{Aut } G$ in this case.
5. The sum of the positive divisors of n is a multiplicative function $\sigma(n)$ similar to $\phi(n)$, satisfying the formula $\sigma(n) = n \prod_{p|n} (1 + \frac{1}{p})$.
- (a) Derive formulas (analogues of Theorems 1.1 and 1.4) expressing n as a sum of values of the σ function, and the reverse.
- (b) A notoriously difficult problem is the determination of solutions of $\sigma(n) = 2n$. Such numbers are called **perfect**. No odd perfect numbers are known. All even perfect numbers have the form $2^{p-1}(2^p - 1)$ where both p and $2^p - 1$ are prime; but only finitely many primes of the form $2^p - 1$ are known (Mersenne primes) although it is conjectured that infinitely many exist. So only finitely many (roughly 50) perfect numbers are known. Say what you can about solutions of the analogous equation $n = 2\phi(n)$.

2. Cyclotomic Polynomials

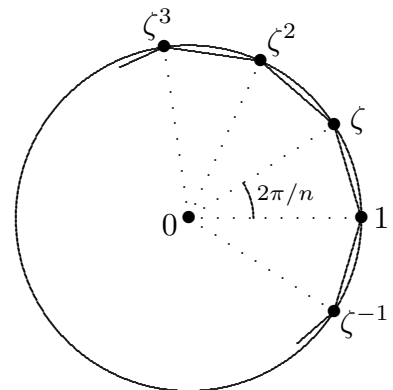
Let n be a positive integer. The multiplicative group \mathbb{C}^\times of units in the complex numbers, form a cyclic group

$$\langle \zeta \rangle = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$$

of order n , where $\zeta = \zeta_n$ is a primitive complex n th root of unity. Usually we take $\zeta_n = e^{2k\pi i/n}$; although for most purposes, any primitive n -th root of unity will serve just as well. We consider $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ as unit vectors in the plane symmetrically arranged about the origin, forming the vertices of a regular n -gon inscribed in the circle $|z|=1$. By symmetry, we directly infer the relation

$$1 + \zeta + \zeta^2 + \dots + \zeta^{n-1} = 0 \quad \text{whenever } n \geq 2,$$

a fact that we can also derive algebraically by comparing coefficients of t^{n-1} on both sides of



$$(2.1) \quad t^n - 1 = (t - 1)(t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{n-1}).$$

So ζ is a root of $1 + t + t^2 + \cdots + t^{n-1} \in \mathbb{Z}[t]$; yet this not in general the minimal polynomial of ζ . The n -th **cyclotomic polynomial** is the monic polynomial defined by

$$\Phi_n(t) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (t - \zeta^k).$$

By construction, its roots are all the $\phi(n)$ primitive n -th roots of unity in \mathbb{C} ; so the coefficients in $\Phi_n(t)$, being the elementary symmetric polynomials in these roots, are algebraic integers. The extension $E = \mathbb{Q}[\zeta] \supseteq \mathbb{Q}$ contains all these roots, since they are powers of ζ ; and so E is the splitting field of $\Phi_n(t)$ over \mathbb{Q} . In particular, $E \supseteq \mathbb{Q}$ is a Galois extension (Appendix A5). Every automorphism $\sigma \in \text{Aut } E$ permutes the roots of $\Phi_n(t)$, so the coefficients in $\Phi_n(t)$ lie in \mathbb{Q} (Theorem A5.12). So by Theorem A3.2(ii), these coefficients must be rational integers. This shows that $\Phi_n(t) \in \mathbb{Z}[t]$.

Grouping together the factors $t - \zeta^r$ in (2.1) according to $\gcd(r, n)$, we have

$$t^n - 1 = \prod_{d|n} \prod_{\substack{1 \leq r \leq n \\ \gcd(r, n) = d}} (t - \zeta^r).$$

Now $\gcd(r, n) = d$ iff $r = dj$ where $1 \leq j \leq \frac{n}{d}$, $\gcd(j, \frac{n}{d}) = 1$. This gives

$$t^n - 1 = \prod_{d|n} \prod_{\substack{1 \leq j \leq \frac{n}{d} \\ \gcd(j, \frac{n}{d}) = 1}} (t - \zeta^{dj}) = \prod_{d|n} \Phi_{\frac{n}{d}}(t)$$

since ζ^{dj} (for $1 \leq j \leq \frac{n}{d}$, $\gcd(j, \frac{n}{d}) = 1$) are the primitive d -th roots of 1. Replacing d by $\frac{n}{d}$ gives part (i) of the following:

Theorem 2.2. (i) For every $n \geq 1$, $t^n - 1 = \prod_{d|n} \Phi_d(t)$.

(ii) Each of the polynomials $\Phi_n(t)$ has integer coefficients; it is irreducible in $\mathbb{Z}[t]$, and so also in $\mathbb{Q}[t]$. Hence $\Phi_n(t)$ is the minimal polynomial of ζ_n over \mathbb{Q} .

The fact that $\Phi_n(t) \in \mathbb{Z}[t]$ was shown above. We have not actually shown that $\Phi_n(t)$ is irreducible in $\mathbb{Z}[t]$ (and so also in $\mathbb{Q}[t]$). Here we give the standard proof of this in the important special case $n = p$ is prime. A similar argument works for prime powers $n = p^e$ (Exercise #2). Lang [L2] proves the irreducibility of $\Phi_n(t)$ in the general case, using an argument which reduces to the prime power case. Now for p prime, use the fact that

$$\Phi_p(t+1) = \frac{(t+1)^p - 1}{t} = t^{p-1} + pt^{p-2} + \frac{p(p-1)}{2}t^{p-2} + \cdots + \frac{p(p-1)}{2}t + p \in \mathbb{Z}[t]$$

where all coefficients (except the leading coefficient) are divisible by p , and the constant term is not divisible by p^2 . By Eisenstein's Criterion (Theorem A2.4), $\Phi_p(t+1) \in \mathbb{Z}[t]$

is irreducible in $\mathbb{Z}[t]$. So $\Phi_p(t) \in \mathbb{Z}[t]$ is also irreducible in $\mathbb{Z}[t]$ (as follows from the substitutions $u = t+1$, $t = u-1$ with all-integer coefficients) and so $\Phi_p(t)$ is also irreducible in $\mathbb{Q}[t]$.

The factorization $t^n - 1 = \prod_{d|n} \Phi_d(t)$ can be reversed to compute the cyclotomic polynomials from the polynomials $t^d - 1$ using ordinary division of polynomials. This may be expressed as

Theorem 2.3. For every $n \geq 1$, $\Phi_n(t) = \prod_{d|n} (t^d - 1)^{\mu(n/d)}$.

For example,

$$\begin{aligned}\Phi_1(t) &= t - 1 \\ \Phi_2(t) &= \frac{t^2-1}{t-1} = t + 1 \\ \Phi_3(t) &= \frac{t^3-1}{t-1} = t^2 + t + 1 \\ \Phi_4(t) &= \frac{t^4-1}{t^2-1} = t^2 + 1 \\ \Phi_5(t) &= \frac{t^5-1}{t-1} = t^4 + t^3 + t^2 + t + 1 \\ \Phi_6(t) &= \frac{(t^6-1)(t-1)}{(t^3-1)(t^2-1)} = t^2 - t + 1 \\ \Phi_7(t) &= \frac{t^7-1}{t-1} = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \\ \Phi_8(t) &= \frac{t^8-1}{t^4-1} = t^4 + 1 \\ \Phi_9(t) &= \frac{t^9-1}{t^3-1} = t^6 + t^3 + 1 \\ \Phi_{10}(t) &= \frac{(t^{10}-1)(t-1)}{(t^5-1)(t^2-1)} = t^4 - t^3 + t^2 - t + 1 \\ &\dots \text{ etc.}\end{aligned}$$

Theorem 2.3 also gives us another proof that $\Phi_n(t) \in \mathbb{Q}[t]$ (leading to another explanation why $\Phi_n(t) \in \mathbb{Z}[t]$). Comparing degrees on both sides of Theorem 2.2(i) gives $n = \sum_{d|n} \phi(d)$; and comparing degrees on both sides of Theorem 2.3 gives $\phi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)d$. So we recover the formulas of Theorems 1.1 and 1.4. Intuition recognizes a connection here; formally, this is expressed by the observation that Theorems 2.2 and 2.3 are **categorified** versions of their counterparts in Section 1. We do not explain the meaning of **categorification**, but it is worth noting that efforts to categorify numerical formulas in a way much like this are often very fruitful.

Theorem 2.4. Let $\zeta = \zeta_n$, $n \geq 1$. Then the extension $E = \mathbb{Q}(\zeta) \supseteq \mathbb{Q}$ is Galois of degree $\phi(n)$. The automorphisms of E form a group $\text{Aut } E = \{\sigma_r : 1 \leq r \leq n, \gcd(r, n) = 1\}$ where $\sigma_r(\zeta) = \zeta^r$. This is an abelian group of order $\phi(n)$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the group of units of the ring of integers mod n . We have $\sigma_r \sigma_s = \sigma_{rs}$ whenever $r, s \in (\mathbb{Z}/n\mathbb{Z})^\times$, so the map $r \mapsto \sigma_r$ is an explicit isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut } E$.

Proof. We have already explained why the extension $E \supseteq \mathbb{Q}$ is the splitting field of $\Phi_n(t)$ over \mathbb{Q} (relying on the fact that $\Phi_n(t)$ is irreducible over \mathbb{Q} , for which we have cited Lang [L2] in the general case). So $E \supseteq \mathbb{Q}$ is Galois of degree $[E : \mathbb{Q}] = \deg \Phi_n(t) = \phi(n)$; and $\text{Aut } E = G(E/\mathbb{Q})$ also has order $\phi(n)$. By Theorems A5.4 and A5.5, G is faithfully represented as a transitive group of permutations of the $\phi(n)$ roots of $\Phi_n(t)$. This gives a representation of G as a group of automorphisms of the cyclic group $\langle \zeta \rangle$ of order n ; and this group has been completely described in the proof of Theorem 1.2. Noting that $\langle \zeta \rangle$ has only these $\phi(n)$ automorphisms, we may identify G with the automorphism group of the cyclic group $\langle \zeta \rangle$ of order n . \square

The general theory of cyclotomic fields will be continued in Section 4. Before then we will quickly survey the theory of finite fields, which will put us in better stead for the sequel.

Exercises 2.

1. Contrary to what one might first guess based on the first few examples, coefficients appearing in cyclotomic polynomials are *not* always 0 or ± 1 . Find the first example (i.e. with the smallest n) in which $\Phi_n(t)$ has a coefficient ± 2 .
2. Let $n = p^e$, p prime, $e \geq 1$. Prove that $\Phi_n(t)$ has integer coefficients and is irreducible in $\mathbb{Z}[t]$, hence also in $\mathbb{Q}[t]$.
3. Let n be a positive integer.
 - (a) Show that $\Phi_{2n}(t) = \begin{cases} t + 1, & \text{for } n = 1; \\ \Phi_n(-t), & \text{for odd } n \geq 3; \\ \Phi_n(t^2), & \text{for } n \text{ even.} \end{cases}$
 - (b) State and prove an analogue of (a) expressing $\Phi_{3n}(t)$ in terms of $\Phi_n(t)$.
 - (c) By generalizing (a) and (b), can you give a formula for $\Phi_{pn}(t)$ in terms of $\Phi_n(t)$ whenever p is prime? If so, does this lead to a practical algorithm for computing cyclotomic polynomials? By ‘practical’, one might ask how well it compares with the algorithm based on Theorem 2.3, and illustrated by the examples which follow that result.
4. Find, with proof, a simple formula for $\Phi_n(1)$.
5. The **general linear group** of degree n over a field F is the multiplicative group $GL_n(F)$ consisting of all invertible $n \times n$ matrices over the field F . In the special case that F is finite with $|F| = q$ elements, one has $|GL_n(\mathbb{F}_q)| = q^{n(n-1)/2} \prod_{k=1}^n (q^k - 1)$. For each $n = 1, 2, \dots, 6$, express $|GL_n(\mathbb{F}_q)|$ as an explicit polynomial in q ; and in each case, factor the resulting polynomial into irreducible factors in $\mathbb{Z}[q]$.

3. Finite Fields

For every prime p , the integers mod p form a field $K = \mathbb{F}_p$. The essential observation here is that every nonzero element $a \in K$ has a multiplicative inverse. (Interpret a as an integer not divisible by p ; then since $\gcd(a, p) = 1$, the extended Euclidean algorithm gives

$1 = ra + sp$ for some $r, s \in \mathbb{Z}$, and then r is an inverse for $a \pmod{p}$.) We next consider *arbitrary* finite fields.

Let F be a finite field; and let $q = |F|$ be its order. Since the additive group of F is finite, every element in this group has finite order; so there is an element $a \in F$ of prime order p in the additive group. Now every nonzero element $b \in F$ must also have additive order p . To see this, note that the map $\theta : F \rightarrow F$, $x \mapsto \frac{a}{b}x$ is clearly bijective and $\theta(x + y) = \theta(x) + \theta(y)$, so θ is an automorphism of the additive group of F ; so b has the same order as $\theta(b) = a$. Thus all nonidentity elements of F have additive order p . An abelian group with this property is **elementary abelian**: it is a direct product of cyclic groups of order p . Thus every finite field F has prime power order $q = p^e$ for some $e \geq 1$ and prime p . Less obvious is the fact that for every prime power q , there is a field F of order q ; and it is unique up to isomorphism, so we may unambiguously write $F = \mathbb{F}_q$. The field F is an extension of degree $[F : K] = e$ over the prime field $K = \mathbb{F}_p$. The prime p is the characteristic of F (and of K). See Appendix A1 for more a general discussion of fields and extensions.

The most direct way to construct $F = \mathbb{F}_q$, $q = p^e$, is to first choose a monic irreducible polynomial $f(t) \in K[t]$ of degree e . Without loss of generality, $f(t)$ is **monic** (its leading coefficient is 1). Then $F = K[\theta]$ where θ is a formal symbol acting as a root of $f(t)$. In other words, $F \cong K[t]/(f(t))$. Now F has $\{1, \theta, \theta^2, \dots, \theta^{e-1}\}$ as a basis over K . This information gives a completely explicit construction of F . (Note that there are p^e monic polynomials in $K[t]$; and at least one of them is irreducible. Take this fact on faith for now; also the fact that the resulting field F doesn't depend on which such irreducible polynomial we choose.)

Example 3.1: The field of order 16. Let $K = \mathbb{F}_2 = \{0, 1\}$. The monic polynomials t and $t+1$ of degree 1 are of course irreducible. Of the four polynomials of degree 2, three (namely t^2 , $t^2+1 = (t+1)^2$ and $t^2+t = t(t+1)$) are reducible; so by process of elimination, the polynomial t^2+t+1 is irreducible. Of the sixteen polynomials of degree 4, we need only consider those with constant term 1 (so that 0 is not a root) and an odd number of terms (so that 1 is not a root). This leaves just four polynomials including $t^4+t^2+1 = (t^2+t+1)^2$; so each of the remaining three choices

$$t^4+t+1, \quad t^4+t^3+1, \quad t^4+t^3+t^2+t+1$$

are all irreducible (because otherwise, an irreducible factor of degree ≤ 2 would be involved, a possibility which we have already ruled out). For simplicity, we take $f(t) = t^4+t+1$ and $F = K[\theta]$ where $f(\theta) = 0$, i.e. $\theta^4 = \theta+1$.

Recall that F^\times is the multiplicative group of order $q-1$ consisting of nonzero elements of F .

Theorem 3.2. Let $F = \mathbb{F}_q$ where $q = p^e$ as above. Then the multiplicative group F^\times is cyclic of order $q-1$.

Proof. By the Fundamental Theorem of Abelian Groups, $F^\times \cong C_{n_1} \times C_{n_2} \times \dots \times C_{n_k}$ as a direct product of cyclic groups of orders n_1, \dots, n_k with $n_1 n_2 \dots n_k = q-1$. In order

to prove that F^\times is itself cyclic, it suffices to prove that $\gcd(n_i, n_j) = 1$ for all distinct i, j . If not, then $\gcd(n_i, n_j) = d \geq 2$ for some $i \neq j$. But then F^\times has at least d^2 elements of order dividing d (inside the subgroup $C_{n_i} \times C_{n_j}$), hence at least $d^2 > d$ roots of the polynomial $x^d - 1$, a contradiction. \square

Example 3.3: The field of order 16. Take $F = \mathbb{F}_{16} = K[\theta]$ where $K = \mathbb{F}_2$ and $\theta^4 = \theta + 1$ as in Example 3.1. Recursively computing $\theta^{j+1} = \theta\theta^j$ gives

$$\begin{array}{cccc} \theta^4 = \theta + 1 & \theta^7 = \theta^3 + \theta + 1 & \theta^{10} = \theta^2 + \theta + 1 & \theta^{13} = \theta^3 + \theta^2 + 1 \\ \theta^5 = \theta^2 + \theta & \theta^8 = \theta^2 + 1 & \theta^{11} = \theta^3 + \theta^2 + \theta & \theta^{14} = \theta^3 + 1 \\ \theta^6 = \theta^3 + \theta^2 & \theta^9 = \theta^3 + \theta & \theta^{12} = \theta^3 + \theta^2 + \theta + 1 & \theta^{15} = 1 \end{array}$$

Of course in the present context (characteristic two), all minus signs are the same as plus signs. Note that the cyclic group F^\times of order 15 contains

- one element 1 of order 1 (the root of $\Phi_1(t) = t - 1$);
- two elements of order 3. These are θ^5 and θ^{10} , the roots of $\Phi_3(t) := t^2 + t + 1$;
- four elements of order 5. These are $\theta^3, \theta^6, \theta^9, \theta^{12}$, the roots of $\Phi_5(t) := t^4 + t^3 + t^2 + t + 1$; and
- eight elements of order 15. These include $\theta, \theta^2, \theta^4, \theta^8$, the roots of $t^4 + t + 1$; and $\theta^7, \theta^{11}, \theta^{13}, \theta^{14}$, the roots of $t^4 + t^3 + 1$. Together these make up the eight roots of $\Phi_{15}(t) = t^8 - t^7 + t^5 - t^4 + t^3 - t + 1$.

The cyclotomic polynomial $\Phi_n(t)$ is defined in Section 2; its roots are the primitive n -th roots of unity. The elements of F are the sixteen roots of $t^{16} - t$; and the elements of F^\times are the fifteen roots of $t^{15} - 1 = \Phi_1(t)\Phi_3(t)\Phi_5(t)\Phi_{15}(t)$.

Squares and Nonsquares

Let $F = \mathbb{F}_q$. If q is even then the map $F \rightarrow F$, $a \mapsto a^2$ is bijective: every element is a square (and every element has a unique square root). This follows from the fact that the group $|F^\times| = q - 1$ has odd order.

Now (and for the remainder of our discussion of squares) assume that q is odd, so that the map $a \mapsto a^2$ on F^\times is two-to-one (since the group F^\times is cyclic of odd order $q - 1$). In this case the subgroup $S \subset F^\times$ of index 2 consists of **squares**; and each element $a^2 \in S$ has exactly two square roots $\pm a \in F$. The cosets of S give a partition $F^\times = S \sqcup N$ where $|S| = |N| = \frac{1}{2}(q - 1)$ and N consists of **nonsquares**. The **quadratic character** of F is the map

$$\chi : F \rightarrow \mathbb{C}, \quad \chi(a) = \begin{cases} 1, & \text{if } a \in S; \\ -1, & \text{if } a \in N; \\ 0, & \text{if } a = 0. \end{cases}$$

Theorem 3.4. For any field F of odd order q , the quadratic character χ satisfies $\chi(a) = a^{\frac{q-1}{2}}$ (interpreted as an element of F). In particular, $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in F$. Thus the product of two squares, or of two nonsquares, is a square; the product of a square and a nonsquare is a nonsquare.

Proof. The assertions are clear when $a = 0$ (or $b = 0$); so assume $ab \neq 0$. The $q - 1$ elements of the cyclic group F^\times are the roots of $t^{q-1} - 1 = (t^{\frac{q-1}{2}} + 1)(t^{\frac{q-1}{2}} - 1)$ where every square $a^2 \in S$ satisfies $(a^2)^{\frac{q-1}{2}} = a^{q-1} = 1$, so the nonzero squares are the $\frac{q-1}{2}$ roots

of $t^{\frac{q-1}{2}} - 1$ in F ; and by elimination, the nonsquares are the roots of $t^{\frac{q-1}{2}} + 1$ in F . The multiplicative property $\chi(ab) = \chi(a)\chi(b)$ follows from the formula $\chi(a) = a^{\frac{q-1}{2}}$. \square

Corollary 3.5. In a field F of odd order q , the element -1 is a square or a nonsquare according as $q \equiv 1$ or $3 \pmod{4}$.

Proof. Use $\chi(-1) = (-1)^{\frac{q-1}{2}}$. \square

We should clarify notation by a simple example: In \mathbb{F}_{13} we might solve $3x + 7 = 2$ by writing $3x = 2 - 7 = -5 = 8$ and $x = \frac{8}{3} = 7$. These equations (not congruences!), although not valid in \mathbb{Q} or in \mathbb{R} , are perfectly valid in the context of \mathbb{F}_{13} ; in particular the expressions $2 - 7$ and $\frac{8}{3}$ are perfectly reasonable (albeit unsimplified) expressions in \mathbb{F}_{13} . Now in a formula such as $\chi(a) = a^{\frac{q-1}{2}}$ where the left side has been defined as $\chi(a) \in \{0, \pm 1\}$ in characteristic zero, while the right side $a^{\frac{q-1}{2}}$ lies in the field F of characteristic p , no confusion should arise as to meaning. In this context, integer values may be interpreted modulo p ; and later, in other contexts, we will treat values of $\chi(a)$ as ordinary integers in characteristic zero.

In fields of odd order, the partition $F = N \sqcup \{0\} \sqcup S$ should be compared with the partition of real numbers as negative, zero, positive; also the remaining assertions of Theorem 3.4 with the fact that a product of two real numbers ab is positive or negative, according as a and b have the same or opposite signs. Since positive and negative real numbers are nonzero squares and nonsquares, the corresponding properties have a common explanation. Yet the analogy is not complete: the sum of two squares in a finite field is not in general a square. This follows necessarily from the fact that there are no finite ordered fields. In fact we have:

Theorem 3.6. Let $a \in F^\times$, $F = \mathbb{F}_q$, q odd, $\varepsilon = (-1)^{\frac{q-1}{2}}$. Then each $s \in S$ has

- (i) $\frac{1}{4}(q-4-\varepsilon)$ solutions of $s = s_1 + s_2$, $(s_1, s_2) \in S \times S$;
- (ii) $\frac{1}{4}(q-2+\varepsilon)$ solutions of $s = s_1 + n_1$, $(s_1, n_1) \in S \times N$; and
- (iii) $\frac{1}{4}(q-\varepsilon)$ solutions of $s = n_1 + n_2$, $(n_1, n_2) \in N \times N$.

Each $n \in N$ has

- (iv) $\frac{1}{4}(q-\varepsilon)$ solutions of $n = s_1 + s_2$, $(s_1, s_2) \in S \times S$;
- (v) $\frac{1}{4}(q-2+\varepsilon)$ solutions of $n = s_1 + n_1$, $(s_1, n_1) \in S \times N$; and
- (vi) $\frac{1}{4}(q-4-\varepsilon)$ solutions of $n = n_1 + n_2$, $(n_1, n_2) \in N \times N$.

Proof. Elementary counting arguments show that the set of triples (a, b, c) with $a, b, c \in F^\times$ and $a + b + c = 0$, form a set \mathcal{T} of size $|\mathcal{T}| = (q-1)(q-2)$. Let m_i be the number

of such triples containing exactly i squares, $i \in \{0, 1, 2, 3\}$. A fixed $\eta \in N$ acts on \mathcal{T} via $(a, b, c) \mapsto (\eta a, \eta b, \eta c)$, showing that $m_{3-i} = m_i$. So

$$2m_2 + 2m_3 = m_0 + m_1 + m_2 + m_3 = |\mathcal{T}| = (q-1)(q-2).$$

Now the $\frac{1}{4}(q-1)^2$ triples $(a, b, -a-b)$ with $a, b \in S$ come in three types:

- (I) m_3 triples with $-a-b \in S$.
- (II) $\frac{1}{3}m_2$ triples with $-a-b \in N$. By symmetry, triples $(a, b, c) \in \mathcal{T}$ containing exactly two squares are equally distributed between $N \times S \times S$, $S \times N \times S$ and $S \times S \times N$.
- (III) Triples with $-a-b = 0$, i.e. $-1 = \frac{a}{b} \in S$. Such triples can only occur if $q \equiv 1 \pmod{4}$, in which case there are $\frac{1}{2}(q-1)$ such triples $(a, -a, 0)$, $a \in S$. In all cases, the number of such triples can be written as $\frac{1}{4}(1+\varepsilon)(q-1)$.

Thus

$$\frac{1}{4}(q-1)^2 = m_3 + \frac{1}{3}m_2 + \frac{1}{4}(1+\varepsilon)(q-1).$$

We now solve to obtain

$$m_0 = m_3 = \frac{1}{8}(q-1)(q-2-3\varepsilon), \quad m_1 = m_2 = \frac{3}{8}(q-1)(q-2+\varepsilon).$$

Now it suffices to prove (i)–(iii), since these yield (iv)–(vi) by simply multiplying each of the equations to be solved by η as above. And in each of (i)–(iii), the number of solutions is independent of the choice of $s \in S$, as follows by multiplying the corresponding equation by s .

For (i), solutions of $1 = s_1 + s_2$ correspond to triples $(1, -s_1, -s_2) \in \mathcal{T}$. There are $\frac{m_3}{(q-1)/2} = \frac{1}{4}(q-5)$ such triples if $\varepsilon = 1$; or $\frac{m_1/3}{(q-1)/2} = \frac{1}{4}(q-3)$ such triples if $\varepsilon = -1$, where $\frac{m_1}{3}$ accounts for threefold symmetry as in (II). In either case we find $\frac{1}{4}(q-4-\varepsilon)$ solutions as claimed in (i).

For (ii), solutions of $1 = s_1 + n_1$ correspond to triples $(1, -s_1, -n_1) \in \mathcal{T}$. Regardless of the value of ε , there are $\frac{m_2/3}{(q-1)/2} = \frac{1}{4}(q-2+\varepsilon)$ such triples.

For (iii), solutions of $1 = n_1 + n_2$ correspond to triples $(1, -n_1, -n_2) \in \mathcal{T}$. There are $\frac{m_1/3}{(q-1)/2} = \frac{1}{4}(q-1)$ such triples if $\varepsilon = 1$; or $\frac{m_3}{(q-1)/2} = \frac{1}{4}(q+1)$ triples if $\varepsilon = -1$. In both cases, the number of solutions is $\frac{1}{4}(q-\varepsilon)$ as claimed in (iii). \square

Automorphisms of Finite Fields

Theorem 3.7. Let $F = \mathbb{F}_q$, $q = p^e$, p prime, $e \geq 1$. Then $\text{Aut } F$ is cyclic of order e , generated by the map $\sigma : F \rightarrow F$, $a \mapsto a^p$. In particular, the extension $F \supseteq K = \mathbb{F}_p$ is Galois, with Galois group $G(F/K) = \{\iota, \sigma, \sigma^2, \dots, \sigma^{e-1}\}$.

Proof. Defining $\sigma : F \rightarrow F$ by $\sigma(a) = a^p$, we clearly have $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in F$. Also

$$\sigma(a + b) = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p = \sigma(a) + \sigma(b)$$

in characteristic p , since all binomial coefficients $\binom{p}{k}$ for $k = 1, 2, \dots, p-1$ are divisible by the prime p . Thus σ is a ring homomorphism. Since F is a field, its only ideals are $\{0\}$ and F ; and $\ker \sigma \neq F$ since $\sigma(1) = 1$. So $\ker \sigma = \{0\}$ and σ is injective. Since F is finite, σ is also bijective, and it is an automorphism of F . The element $\sigma \in \text{Aut } F$ has order at most $e = [F : K]$ by Theorem A5.4(iii). Its order must be exactly e since if $1 \leq k < e$, the nonconstant polynomial $x^{p^k} - x \in K[x]$ cannot have p^e distinct roots. Since the upper bound $|G| = e = [F : K]$ is attained, the extension $F \supseteq K$ is Galois and $G = \langle \sigma \rangle$. \square

A general principle (not actually a theorem) is that almost anything that works for prime order fields, works for finite fields. We now generalize Theorem 3.7 to arbitrary finite fields.

Theorem 3.8. Let $E \supseteq F$ be an extension of finite fields, with $E = \mathbb{F}_{q^n}$, $F = \mathbb{F}_q$, where q is a prime power. Then the extension $E \supseteq F$ is Galois of degree $[E : F] = n$. Its Galois group is cyclic: $G(E/F) = \langle \sigma \rangle = \{\iota, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ where $\sigma(a) = a^q$. The norm and trace maps of the extension are

$$\begin{aligned} N_{E/F}(a) &= \prod_{i=0}^{n-1} \sigma^i(a) = a^{1+q+q^2+\cdots+q^{n-1}}; \\ \text{Tr}_{E/F} a &= \sum_{i=0}^{n-1} \sigma^i(a) = a + a^q + a^{q^2} + \cdots + a^{q^{n-1}}. \end{aligned}$$

Proof. Consider the tower $E \supseteq F \supseteq K$ where $E = \mathbb{F}_{q^n}$, $F = \mathbb{F}_q$, $q = p^e$, $K = \mathbb{F}_p$. By Theorem 3.7, the extension $E \supseteq K$ is Galois of degree ne with group $G = G(E/K) = \langle \tau \rangle$, $\tau(a) = a^p$. Note that $\sigma = \tau^e$ generates the subgroup of order n in G . By Galois correspondence (Theorem A5.11) the fixed field $\text{Fix}_E(\langle \sigma \rangle)$ is the unique subfield of E of order q , so $\text{Fix}_E(\langle \sigma \rangle) = F$. Since $\langle \iota \rangle \leq \langle \sigma \rangle$, the extension $E \supseteq F$ is Galois of degree n and its Galois group is $G(E/F) \cong G_F = \langle \sigma \rangle$. The formulas for norm and trace follow from Theorem A5.13. \square

Polynomials versus Functions

Students encountering finite fields for the first time must come to terms with the revelation that, for example in $\mathbb{F}_3[x]$,

$$(x^2 - 1)^3 = x^6 - 1 \neq x - 1.$$

All three of these polynomials represent the same function $\mathbb{F}_3 \rightarrow \mathbb{F}_3$, namely $0 \mapsto 2 \mapsto 1 \mapsto 0$; and the first two polynomials coincide (since corresponding coefficients agree); but the last two polynomials are distinct (corresponding coefficients do not agree; indeed the two

polynomials don't even have the same degree). In grappling with the source of one's own confusion, the student will come to better understand polynomials and functions, not only over finite fields, but over other fields including \mathbb{R} . The confusion here is not attributable to characteristic; it comes down to a distinction between finite and infinite ground fields. In a nutshell,

Over an infinite field, there are more functions than polynomials;
over a finite field, there are more polynomials than functions.

Let's make sense of this synopsis.

If F is any field, then the set of all functions $F \rightarrow F$ is an algebra over F which we may denote by F^F . Sums, products and scalar multiples of functions are by pointwise evaluation; thus for $f, g \in F^F$, i.e. $f, g : F \rightarrow F$, and scalars $a, b \in F$, the functions $fg : F \rightarrow F$ and $af + bg : F \rightarrow F$ are defined by

$$(fg)(c) = f(c)g(c) \quad \text{and} \quad (af + bg)(c) = af(c) + bg(c) \quad \text{for all } c \in F.$$

Now any polynomial $f(x) \in F[x]$ yields a function $f : F \rightarrow F$ simply by evaluating the polynomial at elements of F . But we must learn in general to distinguish the polynomial $f(x) \in F[x]$ from the resulting function $F \rightarrow F$. When the field F is infinite, the functions representable as polynomials (the so-called **polynomial functions**) form a proper subalgebra of the algebra F^F of all functions $F \rightarrow F$. For example, the function $\mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto \sin x$ is not a polynomial function. One *proves* that over an infinite field F , the polynomial functions form a proper subalgebra of F^F , isomorphic to $F[x]$. This is not an immediate consequence of the definitions; but we will outline a couple of ways to prove it (below).

When the field F is finite, say $|F| = q$, then *every* function $F \rightarrow F$ is representable by a polynomial, but in more than one way. Indeed, there are infinitely many polynomials ($(q-1)q^n$ distinct polynomials of degree n , for each degree $n \geq 0$; plus the zero polynomial) but only finitely many functions ($|F^F| = q^q$ in fact).

To make sense of this, observe that for an arbitrary field F (finite or infinite), every polynomial $f(x) \in F[x]$ can be used to represent a function $f \in F^F$, i.e. $f : F \rightarrow F$. This gives a map which we shall denote by

$$(3.9) \quad \theta : F[x] \rightarrow F^F, \quad f(x) \mapsto f.$$

This map is not only F -linear, it also preserves products; so it is a homomorphism of F -algebras (i.e. vector spaces over F which are also rings). (A little more in fact: since $\theta(1) = 1$, θ is a homomorphism of algebras with identity.) The image of θ is, by definition, the subalgebra of all polynomial functions $F \rightarrow F$. By the First Isomorphism Theorem for Rings,

$$(3.10) \quad F[x]/\ker \theta \cong \{\text{polynomial functions } F \rightarrow F\} \subseteq F^F.$$

Now consider $f(x) \in \ker \theta$, i.e. $f(a) = 0$ for all $a \in F$. If $a_1, a_2, \dots, a_n \in F$ are distinct, then repeated application of the Division Algorithm shows that $f(x)$ is divisible by $(x - a_1)(x - a_2) \cdots (x - a_n)$ in $F[x]$; so either $f(x) = 0$ or $\deg f(x) \geq n$. It follows that for

F infinite, $\ker \theta = 0$, i.e. θ is injective and so each polynomial can be identified with the polynomial function that it represents. On the other hand if $|F| = q$, we see that $\ker \theta \subset F[x]$ is the principal ideal generated by $\prod_{a \in F} (x - a)$. This polynomial of degree $|F| = q$ must actually equal $x^q - x \in F[x]$ which is the unique monic polynomial of degree q having all elements of F as roots, by Theorems 3.7 and 3.8. In summary, we obtain

Theorem 3.11. Let F be a field, and θ as in (3.9).

- (a) If F is infinite, then θ is injective but not surjective; every polynomial $f(x)$ can be safely identified with the resulting function $f = \theta(f(x))$.
- (b) If $|F| = q$, then θ is surjective but not injective; $F^F \cong F[x]/(x^q - x)$; and every function $F \rightarrow F$ can be represented by infinitely many different polynomials, but by a unique polynomial of degree less than q .

As an alternative to the argument above using the Division Algorithm, one can obtain the isomorphism using Lagrange interpolation, which is described as follows.

Theorem 3.12. Let F be a field. Given distinct scalars $a_1, a_2, \dots, a_n \in F$, consider the polynomials

$$f_i(x) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{x - a_j}{a_i - a_j} \in F[x], \quad i \in \{1, 2, \dots, n\}$$

of degree $n - 1$. Then

- (a) $f_i(a_j) = \delta_{i,j}$.
- (b) $f_1(x), f_2(x), \dots, f_n(x)$ form a basis for the n -dimensional subspace of $F[x]$ consisting of all polynomials of degree $< n$.
- (c) Given $b_1, b_2, \dots, b_n \in F$ (not necessarily distinct), the unique polynomial of degree $< n$ whose graph passes through the n points $(a_1, b_1), (a_2, b_2), \dots, (a_n, b_n) \in F^2$ is $a_1 f_1(x) + a_2 f_2(x) + \dots + a_n f_n(x)$. \square

The proof of Theorem 3.12 is elementary; and the basis in 3.12(b) is the **Lagrange interpolation basis**. For $|F| = q$, it shows that every $f : F \rightarrow F$ is represented by a unique polynomial of degree $< q$. This gives an alternative proof of Theorem 3.11.

A third proof of Theorem 3.11 is based on the observation that the problem of constructing a polynomial $f(x) \in F[x]$ whose graph passes through n pairs (a_i, b_i) as in Theorem 3.12, is equivalent to solving a linear system of n equations in n unknowns. The $n \times n$ coefficient matrix of this system is of Vandermonde form and is well known to be invertible. This gives a unique interpolating polynomial.

A final word about obtaining functions from polynomials: Given a polynomial $f(x) \in F[x]$, in addition to the function $f : F \rightarrow F$ represented by $f(x)$, one also obtains a function $E \rightarrow E$ for every extension field $E \supseteq F$. Thus for example, every $f(x) \in \mathbb{Q}[x]$

naturally represents functions $\mathbb{Q} \rightarrow \mathbb{Q}$, $\mathbb{R} \rightarrow \mathbb{R}$, $\mathbb{C} \rightarrow \mathbb{C}$, $\mathbb{Q}[i] \rightarrow \mathbb{Q}[i]$, etc. Returning to the earlier example, although the distinct polynomials $x^6 - 1$ and $x - 1$ in $\mathbb{F}_3[x]$ represent the same function $\mathbb{F}_3 \rightarrow \mathbb{F}_3$, they represent distinct functions over $\mathbb{F}_9 \rightarrow \mathbb{F}_9$. Given two polynomials $f(x), g(x) \in F[x]$ where F is a finite field, we have that $f(x) = g(x)$ iff the two polynomials represent the same function $\overline{F} \rightarrow \overline{F}$, where $\overline{F} \supset F$ is the algebraic closure.

Counting Irreducible Polynomials

Let $F = \mathbb{F}_q$. Denote by $n_{q,d}$ (or simply n_d , since q will usually remain unchanged throughout our discussion) the number of monic irreducible polynomials $f(x) \in F[x]$ of degree $d \geq 1$. In the construction of finite fields, we make essential use of the fact that $n_d \geq 1$ for all d . Here we give a formula for n_d , from which it follows that for a monic polynomial $f(x) \in F[x]$ of degree d chosen uniformly at random, the probability that $f(x)$ is irreducible is asymptotically $\frac{1}{d}$ as $d \rightarrow \infty$. The total number of elements in \mathbb{F}_{q^k} is

$$q^k = \sum_{d|k} dn_d$$

since each $\alpha \in \mathbb{F}_{q^k}$ is algebraic of some degree $d \mid k$; and the minimal polynomial of α over F has d distinct roots in this extension. It follows (by induction on d , or by Möbius inversion, or by inclusion-exclusion; cf. Section 1) that

$$kn_k = \sum_{d|k} \mu\left(\frac{k}{d}\right) q^d = \sum_{d|k} \mu(d) q^{\frac{k}{d}}.$$

This may be rewritten as conclusion (ii) of:

Theorem 3.13. The number n_k of monic irreducible polynomials $f(x) \in \mathbb{F}_q[x]$ of degree k satisfies

(i) $q^d = \sum_{k|d} kn_k$; and

(ii) $n_k = \frac{1}{k} \sum_{d|k} \mu(d) q^{\frac{k}{d}} = \frac{q^k}{k} \prod_{\text{prime } r|k} \left(1 - \frac{1}{q^{(1-\frac{1}{r})k}}\right) \sim \frac{q^k}{k}$ as $k \rightarrow \infty$.

Notice, by the way, that this formula asserts that $n_k > 0$ for all $k \geq 1$. (However, our argument cannot be construed as proof of the existence of irreducible polynomials of every degree, if one first assumes the existence of $\mathbb{F}_q^k \cong \mathbb{F}_q[x]/(m(x))$ obtained using an irreducible polynomial $m(x) \in \mathbb{F}_q[x]$ of degree k , as this would constitute circular reasoning. One could however obtain the same formula by counting polynomials of each degree instead of counting elements of each degree.)

The following result will be required in Sections 13 and 14. It is a fundamental result in finite projective geometry (see [M4]); but in keeping with the scope of this course, here we state and prove it in the affine setting.

Theorem 3.14 (Segre). Let $f : F \rightarrow F$ where $F = \mathbb{F}_q$ is a finite field of *odd* order q . Then the following conditions are equivalent.

- (i) There exist $a, b, c \in F$ with $a \neq 0$ such that $f(x) = ax^2 + bx + c$ for all $x \in F$.
- (ii) No three points of the graph of f (the point set $\Gamma_f = \{(x, f(x)) : x \in F\} \subset F^2$) are collinear.

Proof. Clearly (i) implies (ii). Points of intersection of the graphs of $y = f(x)$ and $y = mx + k$ ($m, k \in F$) are found by first solving $ax^2 + bx + c = mx + k$ for x ; this has at most two solutions for $x \in F$ and hence at most two points of intersection (x, y) .

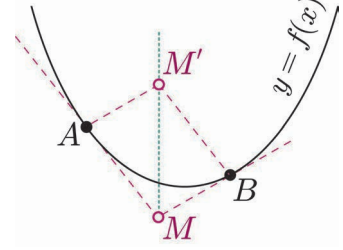
Conversely, suppose f satisfies (ii). The following observation will be useful later.

- (3.15) We may freely apply an affine linear transformation $T : F^2 \rightarrow F^2$ of the form $T(x, y) = (\alpha x + \beta, \gamma y + \delta)$ $\alpha, \beta, \gamma, \delta \in F$ with $\alpha\delta \neq 0$ to Γ_f without altering either the hypothesis (ii) or the desired conclusion (i). In other words, f satisfies (i) (respectively, (ii)) iff the variant $x \mapsto \gamma f\left(\frac{x-\beta}{\alpha}\right) + \delta$ satisfies (i) (respectively, (ii)).

Each point $P = (x_0, f(x_0))$ lies on $q-1$ secant lines passing through the other points $(x, f(x))$ of Γ_f , $x \neq x_0$; and by (ii), these $q-1$ secants are necessarily distinct. Since there are exactly q non-vertical lines through P (corresponding to the q choices from F for the slope), each point $P \in \Gamma_f$ lies on a unique **tangent** line, this being the unique non-vertical line intersecting Γ_f in the unique point P . Now Γ_f has q tangent lines, and it is not hard to see that any two tangent lines differ in slope. (Consider the tangent line ℓ through a point $P \in \Gamma_f$, and let $Q \neq P$ be another point of ℓ . Since $|\Gamma_f| = q$ is odd and every line through Q meets Γ_f in 0, 1 or 2 points, there must be an even number of tangent lines passing through Q (remembering that the vertical line through Q is not considered here as a tangent line). Since Q already lies on ℓ , each of the $q-1$ points $Q \neq P$ on ℓ must lie on at least one additional tangent line other than ℓ . Since each of the $q-1$ tangent lines $\ell' \neq \ell$ meets ℓ in a single point (since ℓ' and ℓ have different slope), the Pigeonhole Principle shows that each point $Q \neq P$ on ℓ lies on a unique tangent line other than P . This verifies our claim that *no point of the plane F^2 lies on more than two tangent lines.*

At this point we prove the following fact, which is usually known as the **Lemma of Tangents**.

(3.16) Let $A \neq B$ be distinct points in Γ_f , and let M be the point of intersection of their corresponding tangent lines. Then the x -coordinate of M is the average of the x -coordinates of A and B . (Stated geometrically, if we complete the parallelogram $AMB M'$ as shown, then the diagonal MM' is vertical.)



Note that if A, M, B have coordinates $(a_1, a_2), (m_1, m_2), (b_1, b_2)$ respectively, then the assertion of (3.16) is that $m_1 = \frac{a_1 + b_1}{2}$. This formula makes sense only because $\text{char } F$ is odd (see Exercise #2 regarding the situation in even characteristic). Put another way, in fields of even characteristic, no arithmetic progression can have more than two distinct terms.

Proof of (3.16). By (3.15), there is no loss of generality in assuming that the points A and B have coordinates $(0, 0)$ and $(1, 0)$ respectively. (The transformations in (3.15) not only preserve the properties (i) and (ii); they also preserve the property described by the conclusion of (3.16).) Denote by $f'(x)$ the slope of the tangent line to Γ_f at the point $(x, f(x))$. (Of course f' is simply a convenient name to use here; it is not intended to connote differentiation. Note that $f'(0) \neq 0$ since the tangent line at A cannot pass through B ; and likewise, $f'(1) \neq 0$.) The points $P(x, f(x)) \in \Gamma_f$ other than A, B are indexed by the values $x \in F, x \neq 0, 1$; and each such point determines two secant lines PA, PB with nonzero slopes $\frac{f(x)}{x}$ and $\frac{f(x)}{x-1}$ respectively. Now consider the product

$$\Pi = \prod_{\substack{P \in \Gamma_f \\ P \neq A, B}} \frac{\text{slope of } PA}{\text{slope of } PB}$$

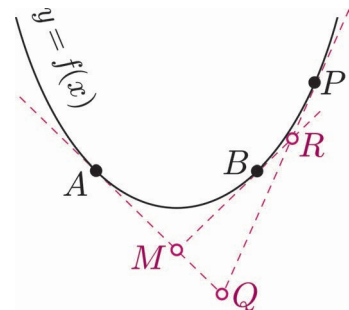
having $q-2$ factors in the numerator, including all of the nonzero elements of F *except* $f'(0)$ (since only three lines through A have been omitted: the horizontal and vertical line, and the tangent line). Similarly, the denominator of Π includes all of the nonzero elements of F *except* $f'(1)$ (the slope of the tangent line through B). After cancelling like factors, we obtain $\Pi = \frac{f'(1)}{f'(0)}$. However, the preceding expressions for the slopes of PA and PB give

$$\Pi = \prod_{\substack{P \in \Gamma_f \\ P \neq A, B}} \frac{\text{slope of } PA}{\text{slope of } PB} = \prod_{\substack{x \in F \\ x \neq 0, 1}} \frac{f(x)/x}{f(x)/(x-1)} = \prod_{\substack{x \in F \\ x \neq 0, 1}} \frac{x-1}{x} = -1$$

since in the latter product, the only element of F^\times omitted in the numerator is -1 , whereas the denominator omits only 1 as a factor. Equating these two expressions for Π yields $f'(0) = -f'(1) = m$ for some $m \in F^\times$. This means that M is the point $(\frac{1}{2}, \frac{m}{2})$, which completes the proof of (3.16).

Now to complete the proof of Theorem 3.14, still assuming (ii) holds, we fix two points A, B in Γ_f . We will henceforth assume (without loss of generality, using (3.15)) that these

are the points $(-1, 1)$ and $(1, 1)$ respectively; and that the point M where their tangents meet is the point $(0, -1)$. (Recall that $-1 \neq 1$ since q is odd. These coordinates differ from the choices in our proof of (3.16); but our new choices benefit from a different use of symmetry.) Consider an arbitrary point $P(x, f(x)) \in \Gamma_f$ distinct from A and B . Denote by Q and R the points where the tangent at P meets the tangent lines through A and B , respectively. By (3.15), these points have coordinates $Q = (\frac{x-1}{2}, u)$ and $R = (\frac{x+1}{2}, v)$ for some $u, v \in F$. Since A, M, Q are collinear, we must have $u = -x$; and collinearity of B, M, R requires $v = x$. Finally, the collinearity of P, Q, R requires $f(x) = x^2$. \square



We remark that in the projective setting, the three lines AR , BQ and PM all pass through a common point O ; and this assertion is the more general form of the Lemma of Tangents. In affine coordinates as above, assuming $x^2 - x + 1 \neq 0$, one finds that $O = (\frac{x(x+1)}{2(x^2-x+1)}, \frac{1}{2(x^2-x+1)})$. This is not a problem except when $q = 3^e$ and $x = -1$; or when $q \equiv 1 \pmod{6}$ and x is a primitive sixth root of unity in F (see Exercise #10.2). In these cases O lies ‘at infinity’ and then the appropriate affine description is that the lines AR , BQ and PM are mutually parallel. The traditional proof of Segre’s Theorem includes the full version of the Lemma of Tangents, as is most natural in the projective setting. But our proof above suffices because the complete statement of the Lemma of Tangents is ... er ... tangential to the immediate goal of proving Segre’s Theorem. While (3.15) is itself a special case of the Lemma of Tangents, this however is easily stated in affine form.

Since we will use of Segre’s Theorem in Section 13 to prove something about cyclotomic fields, it is appropriate to question whether the geometric terminology of Segre’s Theorem should be required to prove an essentially algebraic fact. Our personal view is that the geometric language and figures used here provide a conceptual aid which is surely helpful in following the proof. While the pictures might not be strictly necessary, the finiteness of F (enabling us to use the Pigeonhole Principle) was indispensable.

Exercises 3.

1. (a) The proof of (3.16) involves the product of all $q-1$ nonzero elements of the finite field $F = \mathbb{F}_q$. Prove that this product equals -1 . (Our proof did not require the explicit value of this product, because almost all factors in the top and bottom of Π were cancelled.) *Hint:* For each factor x in $\prod_{x \neq 0} x$, the factor x^{-1} also appears.
- (b) As a corollary, obtain **Wilson’s Theorem**: $(p-1)! \equiv -1 \pmod{p}$ for every prime p .

2. Let F be a finite field of even order $q = 2^e$. (Keep in mind that for fields of even order, the map $a \mapsto a^2$ is an automorphism, by Theorem 3.7. Its inverse, $a \mapsto \sqrt{a}$, is also an automorphism. Thus every element has a unique square root; and $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$, $\sqrt{ab} = \sqrt{a}\sqrt{b}$.) Consider the function $f : F \rightarrow F$ defined by $f(a) = \frac{1}{a}$, if $a \neq 0$; $f(0) = 0$.
 - (a) Show that no three points of the graph of f are collinear. (Compare with Theorem 3.14(ii).)
 - (b) Show that the graph of f is represented by a quadratic polynomial (as in Theorem 3.14(i)) for $q \in \{2, 4\}$, but not for $q \geq 8$. This shows the failure of Segre's Theorem in even characteristic.
3. Consider an extension $E \supseteq F$ of finite fields of odd order, and consider a nonzero element $a \in E^\times$. Show that a is a square in E iff its norm $N_{E/F}(a)$ is a square in F . ('Square in E ' means an element of the form b^2 , $b \in E$. 'Square in F ' means an element of the form b^2 , $b \in F$.)
4. Let F be a finite field.
 - (a) Show that every subring of F is a subfield.
 - (a) Show that the conclusion in (a) does not hold without the hypothesis that the field F is finite.
5. Factor each of the following cyclotomic polynomials into irreducible factors in $\mathbb{F}_{13}[t]$:
 - (a) $\Phi_4(t)$ (b) $\Phi_5(t)$ (c) $\Phi_6(t)$ (d) $\Phi_8(t)$
6. Let $F = \mathbb{F}_q$ be a finite field, and let $n \geq 1$.
 - (a) Show that every root of $\Phi_n(t)$ in F is a primitive n th root of unity in F .
 - (b) Show that $\Phi_n(t)$ has a root in F iff $\Phi_n(t)$ splits into linear factors in $F[t]$, iff $q \equiv 1 \pmod{n}$.
7. Give explicit formulas for $n_{q,d}$, the number of irreducible polynomials in $\mathbb{F}_q[x]$ of degree $d \in \{1, 2, 3, 4, 5\}$.

4. Cyclotomic Fields and Integers

Let n be a positive integer. As before, $\zeta = \zeta_n$ is a primitive n -th root of unity in \mathbb{C} , i.e. an element of order n in \mathbb{C}^\times . Thus $\zeta^n = 1$ and n is the smallest positive integer with this property. There are $\phi(n)$ such primitive n -th roots of unity in \mathbb{C} , these being the values ζ^k for $1 \leq k \leq n$, $\gcd(k, n) = 1$. For *most* purposes (we will encounter some exceptions), the primitive roots are interchangeable: it does not matter which of these values we take to be ζ . The standard choice, however, is $\zeta_n = e^{2\pi i/n}$. The field $E = \mathbb{Q}[\zeta]$ is a **cyclotomic field**.

Recall that the automorphisms of E form the Galois group $G = \{\sigma_k : \gcd(k, n) = 1\} \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the group of units of the ring of integers mod n . Here $\sigma_k(\zeta) = \zeta^k$; and the map $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow G$, $k \mapsto \sigma_k$ is an isomorphism. In particular, $\sigma_k \sigma_\ell = \sigma_{k\ell} = \sigma_\ell \sigma_k$, and so G is abelian.

An **abelian extension** is a Galois extension whose Galois group is abelian. So cyclotomic extensions are abelian. More generally, every Galois extension $F \supseteq \mathbb{Q}$ contained in a cyclotomic extension (i.e. $E \supseteq F \supseteq \mathbb{Q}$) must also be abelian, by Galois theory (since $\text{Aut } F$ is a subgroup of an abelian group $\text{Aut } E$), and this simple fact has an important converse: *Every abelian extension of \mathbb{Q} is contained in a cyclotomic field.* This result,

known as the **Kronecker-Weber Theorem**, indicates clearly the very special nature of cyclotomic extensions; but its proof is beyond the scope of our course. See [Wa], [L1] for details.

An important consequence of the fact that cyclotomic extensions are abelian, is

Theorem 4.1. For every automorphism $\sigma \in \text{Aut } E$ of a cyclotomic extension $E = \mathbb{Q}[\zeta]$, and every $z \in E$, we have $\sigma(\bar{z}) = \overline{\sigma(z)}$.

Be warned that this is a special property not valid in most Galois extensions! See Examples A5.8 and A5.10, for two instances where $\sigma\tau \neq \tau\sigma$; and τ is complex conjugation in each of those examples.

Proof of Theorem 4.1. Denote by $\tau \in \text{Aut } E$ the complex conjugation map $\tau(z) = \bar{z}$. Since $\text{Aut } E$ is abelian, we have $\sigma\tau(z) = \tau\sigma(z)$. (In fact, $\tau = \sigma_{-1}$. So if $\sigma = \sigma_k$, then $\sigma\tau = \sigma_{-k} = \tau\sigma$.) \square

We should next proceed by describing the other important features of cyclotomic fields: classify the ring of algebraic integers $\mathcal{O} \subset E$, the unit group \mathcal{O}^\times , some facts about irreducibles and factorization in \mathcal{O} , etc. All of this will require some work, and we will have to take many of the key results on faith (with some references provided). We will however be able to include proofs of several of the key results. Let's start, however, with some low-hanging fruit.

It is easy to see exactly how many roots of unity $\mathbb{Q}[\zeta]$ has:

Theorem 4.2. The roots of unity in $\mathbb{Q}[\zeta_n]$ form a cyclic group $\langle \zeta_n \rangle$ of order n , if n is even; or $\langle \zeta_{2n} \rangle$ of order $2n$ if n is odd.

Proof. Without loss of generality, n is even; since for odd n , the field $\mathbb{Q}[\zeta_n]$ already contains a primitive $2n$ -th root of unity $-\zeta_n$. Now given a primitive m -th root of unity ζ_m in $\mathbb{Q}[\zeta_n]$, we must show that ζ_m is a power of ζ_n , i.e. that m divides n . Suppose not; then there exists a prime power p^d , p prime, $d \geq 1$, dividing m but not dividing n . Without loss of generality $m = p^d$; otherwise replace ζ_m by ζ_m^{m/p^d} , a primitive p^d -th root of unity in $\mathbb{Q}[\zeta_n]$. Let $n' = \text{lcm}(m, n) = p^{d-k}n$ where p^k is the largest power of p dividing n , and $d - k \geq 1$. Clearly $\zeta_m\zeta_n$ is a primitive n' -th root of unity in $E = \mathbb{Q}[\zeta_n]$, so that $E \supseteq \mathbb{Q}[\zeta_{n'}] \supseteq \mathbb{Q}$ and $\phi(n') | \phi(n)$. However, $\phi(n') = p^{d-k}\phi(n) > \phi(n)$ by Section 1, a contradiction. \square

Since $\mathbb{Q}[\zeta_n] = \mathbb{Q}[\zeta_{2n}]$ whenever n is odd (where we may take $\zeta_{2n} = -\zeta_n$), and in order to avoid the exceptional alternative of Theorem 4.2, we will often want to assume that n is even.

Since $\zeta = \zeta_n$ is a root of unity, it is in particular an algebraic integer; and since the algebraic integers form a subring $\mathcal{O} \subset \mathbb{Q}[\zeta]$, we must have $\mathbb{Z}[\zeta] \subseteq \mathcal{O} \subset \mathbb{Q}[\zeta]$. Actually, equality holds in general: $\mathcal{O} = \mathbb{Z}[\zeta]$, although we give the details only for prime values of n (see Theorem 4.5).

Determining the full group of units \mathcal{O}^\times takes a little more work. Clearly the roots of unity (as in Theorem 4.2) form a subgroup of \mathcal{O}^\times , namely the torsion subgroup of \mathcal{O}^\times . Some additional units are found as follows:

Theorem 4.3. Let $\zeta = \zeta_n$, $n \geq 2$; and suppose $r, s \in \mathbb{Z}$ with $\gcd(rs, n) = 1$. Then $\frac{1-\zeta^r}{1-\zeta^s}$ is a unit.

Proof. Since r and s are relatively prime, ζ^r and ζ^s are primitive n -th roots of unity, so each of them is a power of the other. (We must remark that $\zeta^r \neq 1$ and $\zeta^s \neq 1$ since $n \geq 2$.) In particular, $\zeta^s = (\zeta^r)^k$ for some integer k . Thus

$$1 - \zeta^s = 1 - \zeta^{kr} = (1 - \zeta^r)(1 + \zeta^r + \zeta^{2r} + \cdots + \zeta^{(k-1)r}) = (1 - \zeta^r)u$$

where $u \in \mathcal{O}$. Similarly, $1 - \zeta^r = (1 - \zeta^s)v$ where $v \in \mathcal{O}$. Since $uv = 1$, u and v are units in \mathcal{O} . \square

Theorem 4.4. For $\zeta = \zeta_p$, p prime, the element $\varepsilon = 1 - \zeta$ is irreducible of norm p . The rational prime p ramifies as $(p) = (\varepsilon)^{p-1}$ in \mathcal{O} , the ring of integers in \mathcal{O} .

Proof. Evaluating $\Phi_p(x) = (x - \zeta)(x - \zeta^2)(x - \zeta^3) \cdots (x - \zeta^{p-1})$ at 1 yields $p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}) = u\varepsilon^{p-1}$ for some unit $u \in \mathcal{O}^\times$, by Theorem 4.3. This yields the equality of ideals $(p) = (\varepsilon)^{p-1}$ in \mathcal{O} . Since the factors $1 - \zeta^i$ ($i = 1, 2, \dots, p-1$) are the algebraic conjugates of $\varepsilon = 1 - \zeta$ by Theorem 2.4, the norm of ε is $N_{E/\mathbb{Q}}(\varepsilon) = p$ by Theorem A5.13.

If $\varepsilon = ab$ where $a, b \in \mathcal{O}$, then $p = N(\varepsilon) = N(a)N(b)$ where $N(a), N(b) \in \mathbb{Z}$, so without loss of generality $N(a) = \pm 1$ and $N(b) = \pm p$ (otherwise interchange a and b). But then $\pm 1 = N(a) = aa'$ where $a' = \prod_{k=2}^{p-1} \sigma_k(a) \in \mathcal{O}$, which shows that $a \in \mathcal{O}^\times$. Thus ε is irreducible in \mathcal{O} . \square

We have mentioned the following result, found in [Wa, Theorem 2.6] with proof relying on [L2, p.68]. We give the proof only in the important case that n is prime.

Theorem 4.5. For $\zeta = \zeta_n$, the ring of integers $\mathcal{O} \subset \mathbb{Q}[\zeta]$ is given by $\mathcal{O} = \mathbb{Z}[\zeta]$.

Proof of Theorem 4.5 for $n = p$ prime. Let $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2} \in \mathcal{O}$ where $a_i \in \mathbb{Q}$; we must show that each $a_i \in \mathbb{Z}$. We first show that no primes occur in the denominators of the coefficients a_i , other than possibly p . For each $\sigma_k \in \text{Aut } E$ (in the notation of Theorem 2.4, where $k = 1, 2, \dots, p-1$), evidently $\alpha_k := \sigma_k(\alpha)$ is also an algebraic integer. This gives a linear system

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_{p-1} \end{bmatrix} = \begin{bmatrix} 1 & \zeta & \zeta^2 & \cdots & \zeta^{p-2} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-2)} \\ 1 & \zeta^3 & \zeta^6 & \cdots & \zeta^{3(p-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-2)(p-1)} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-2} \end{bmatrix} = M \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{p-2} \end{bmatrix}$$

in which the coefficient matrix M is a Vandermonde matrix of order $p-1$. Its determinant, as found by a well-known formula, is

$$\det M = \prod_{1 \leq i < j \leq p-1} (\zeta^j - \zeta^i) = u(1 - \zeta)^k$$

for some $u \in \mathcal{O}^\times$ by Theorem 4.3 and $k = \binom{p-1}{2} \geq 0$. Now

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{p-2} \end{bmatrix} = M^{-1} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{p-1} \end{bmatrix}$$

so each $a_i = a'_i/\varepsilon^k$ for some $a'_i \in \mathcal{O}$. Since $p = \varepsilon^{p-1}$, there exists a positive integer m such that $p^m a_i \in \mathcal{O}$ for all $i \in \{0, 1, 2, \dots, p-2\}$. However, $p^m a_i \in \mathbb{Q}$. By Theorem A3.2(ii), $p^m a_i \in \mathbb{Z}$ and so $p^m \alpha \in \mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta] = \mathbb{Z}[\varepsilon]$; we may write

$$\varepsilon^{(p-1)m} \alpha = p^m \alpha = b_0 + b_1\varepsilon + b_2\varepsilon^2 + \cdots + b_{p-2}\varepsilon^{p-2}, \quad b_i \in \mathbb{Z}.$$

We need to show that $\alpha \in \mathbb{Z}[\zeta] = \mathbb{Z}[\varepsilon]$, so without loss of generality $m \geq 1$ and suppose at least one of the b_i is not divisible by p ; we seek a contradiction. Let $k \in \{0, 1, 2, \dots, p-2\}$ be *minimal* such that $b_k \not\equiv 0 \pmod{p}$. Note that $\sum_{i=0}^{p-2} b_i \varepsilon^i \notin (\varepsilon)^{k+1}$ since $b_k \varepsilon^k \notin (\varepsilon)^{k+1}$ but all other terms lie in $(\varepsilon)^{k+1}$. However, $p^m \alpha \in (p) \subseteq (\varepsilon)^{k+1}$, a contradiction as desired. \square

Discriminants and their use are discussed in Appendix A3. For the prime $p = 2$, note that $\mathbb{Z}[\zeta_2] = \mathbb{Z}[-1] = \mathbb{Z}$ which has discriminant 1. The discriminant of $\mathbb{Z}[\zeta_n]$ for general $n \geq 2$ is

$$(-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}};$$

see [Wa, Chapter 2].

Theorem 4.6. Suppose $\zeta = \zeta_p$, p an odd prime. Then the discriminant of $\mathcal{O} = \mathbb{Z}[\zeta]$ is $(-1)^{\frac{p-1}{2}} p^{p-2}$; and the only rational prime that ramifies in $E = \mathbb{Q}[\zeta]$ is p .

Proof. For $k \not\equiv 0 \pmod{p}$, ζ^k is a primitive p -th root of unity, and its algebraic conjugates are $\zeta, \zeta^2, \dots, \zeta^{p-1}$ so $\text{Tr}_{E/\mathbb{Q}}(\zeta^k) = \zeta + \zeta^2 + \dots + \zeta^{p-1} = -1$; whereas if $k \equiv 0 \pmod{p}$, then $\zeta^k = 1$ and $\text{Tr}_{E/\mathbb{Q}}(\zeta^k) = 1+1+\dots+1 = p-1$. In view of the relation $1+\zeta+\zeta^2+\dots+\zeta^{p-1} = 0$, any $p-1$ of the elements $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ form a base for $\mathbb{Z}[\zeta]$ over \mathbb{Z} . It is convenient for us to use $\zeta, \zeta^2, \zeta^3, \dots, \zeta^{p-1}$ as our choice of base. As described in Appendix A3,

$$\begin{aligned} \text{disc}(\zeta, \zeta^2, \dots, \zeta^{p-1}) &= \det[\text{Tr}_{E/\mathbb{Q}}(\zeta^i \zeta^j) : 1 \leq i, j \leq p-1] \\ &= \det \begin{bmatrix} -1 & -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & -1 & \cdots & -1 & p-1 \\ -1 & -1 & -1 & \cdots & p-1 & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & -1 & p-1 & \cdots & -1 & -1 \\ -1 & p-1 & -1 & \cdots & -1 & -1 \end{bmatrix} \quad ((p-1) \times (p-1) \text{ matrix}) \\ &= \det \begin{bmatrix} -1 & -1 & -1 & \cdots & -1 & -1 \\ 0 & 0 & 0 & \cdots & 0 & p \\ 0 & 0 & 0 & \cdots & p & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & p & \cdots & 0 & 0 \\ 0 & p & 0 & \cdots & 0 & 0 \end{bmatrix} = (-1)^{\frac{p-1}{2}} p^{p-2}. \end{aligned}$$

Since the only rational prime dividing the discriminant is p , the result follows from Appendix A3 (the remarks about ramification following Theorem A3.10). \square

Example 4.7: The Cyclotomic Field $\mathbb{Q}[\zeta_3]$. Let $E = \mathbb{Q}[\zeta_3]$. Our primitive cube root of unity is $\zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$. By Theorem 4.6, E has discriminant -3 . Since $E \supset \mathbb{Q}$ is an imaginary quadratic extension, this is covered by Example A3.5 where the same value -3 is found for the discriminant. See also Example A3.8 regarding this extension.

The **maximal real subfield** of $\mathbb{Q}[\zeta]$ is the subfield $\mathbb{R} \cap \mathbb{Q}[\zeta]$. It is often denoted by $\mathbb{Q}[\zeta]^+$.

Theorem 4.8. The maximal real subfield of $E = \mathbb{Q}[\zeta]$, $\zeta = \zeta_n$, $n \geq 3$, is $F = \mathbb{Q}[\zeta] \cap \mathbb{R} = \mathbb{Q}[\alpha]$ where $\alpha = \zeta + \zeta^{-1}$, an algebraic integer of degree $\frac{1}{2}\phi(n)$. The ring of integers of F is $\mathbb{Z}[\zeta] \cap \mathbb{R} = \mathbb{Z}[\alpha]$.

Proof. Let $E = \mathbb{Q}[\zeta]$ and $F = \mathbb{Q}[\alpha]$, $\alpha = \zeta + \zeta^{-1}$. Since $\alpha = \zeta + \bar{\zeta} \in \mathbb{R}$ but $\zeta \notin \mathbb{R}$, $[E : F] \geq 2$. Since $\alpha\zeta = \zeta^2 + 1$, ζ is a root of $f(x) = x^2 - \alpha x + 1 \in F[x]$, so $[E : F] \leq 2$. This forces $[E : F] = 2$. Also since $E \subseteq E \cap \mathbb{R} \subset E$, $[E \cap \mathbb{R} : F]$ is a proper divisor of $[E : F] = 2$, which forces $[E \cap \mathbb{R} : F] = 1$, so $F = E \cap \mathbb{R}$. Also $\phi(n) = [E : \mathbb{Q}] = [E : F][F : \mathbb{Q}] = 2[F : \mathbb{Q}]$, so $[\mathbb{Q}[\alpha] : \mathbb{Q}] = [F : \mathbb{Q}] = \frac{1}{2}\phi(n)$. This shows, of course, that α is algebraic of degree $\frac{1}{2}\phi(n)$.

There is however a more direct interpretation of this value $\frac{1}{2}\phi(n)$ using two explicit bases for $\mathbb{Q}[\alpha]$ over \mathbb{Q} . The obvious basis is $\{\alpha^k : 0 \leq k < \frac{1}{2}\phi(n)\}$. Another basis consists of the algebraic integers

$$\alpha_k = \begin{cases} 1, & \text{for } k = 0; \\ \zeta^k + \zeta^{-k}, & \text{for } k = 1, 2, \dots, \frac{1}{2}\phi(n) - 1. \end{cases}$$

Note that $\alpha_1 = \alpha$; and for each k in the indicated interval, the binomial expansion gives

$$\alpha^k = \begin{cases} \sum_{0 \leq i \leq \frac{k-1}{2}} \binom{k}{i} \alpha_{k-2i}, & \text{for } k \text{ odd;} \\ \binom{k}{k/2} + \sum_{0 \leq i \leq \frac{k-2}{2}} \binom{k}{i} \alpha_{k-2i}, & \text{for } k \text{ even.} \end{cases}$$

Induction shows that $\{\alpha_0, \alpha_1, \dots, \alpha_k\}$ and $\{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^k\}$ span the same \mathbb{Q} -subspace of $\mathbb{Q}[\alpha]$ for each k . In fact by the relations above, the change-of-basis matrix between the two bases is upper triangular. Indeed, since the change-of-basis matrix has integer entries with 1's on the main diagonal, it follows that $\{\alpha_0, \alpha_1, \dots, \alpha_k\}$ and $\{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^k\}$ span the same \mathbb{Z} -submodule of $\mathbb{Z}[\alpha]$ for each k .

Now suppose $\beta \in \mathbb{Q}[\alpha]$ is an algebraic integer; we must show that $\beta \in \mathbb{Z}[\alpha]$. Simply express

$$\beta = \sum_{k=0}^{N-1} b_k \alpha_k = b_0 + \sum_{k=1}^{N-1} b_k (\zeta^k + \zeta^{-k})$$

where $b_k \in \mathbb{Q}$ for $k = 0, 1, 2, \dots, N-1$; $N = \frac{1}{2}\phi(n) - 1$. In order that β be an algebraic integer, Theorem 4.5 requires each $b_k \in \mathbb{Z}$; but then the observations above indicate that β is a \mathbb{Z} -linear combination of $\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{N-1}$, i.e. $\beta \in \mathbb{Z}[\alpha]$. \square

Example 4.9: The Maximal Real Subfield of $\mathbb{Q}[\zeta_7]$. Let $\zeta = \zeta_7$, $\alpha = \zeta + \zeta^{-1}$, $\alpha^2 = \zeta^2 + \zeta^{-2} + 2$, $\alpha^3 = \zeta^3 + \zeta^{-3} + 3(\zeta + \zeta^{-1})$. We have

$$\begin{aligned} \alpha^3 + \alpha^2 - 2\alpha^2 - 1 &= \zeta^3 + \zeta^{-3} + 3(\zeta + \zeta^{-1}) + \zeta^2 + \zeta^{-2} + 2 - 2(\zeta + \zeta^{-1}) - 1 \\ &= \zeta^3 + \zeta^{-3} + \zeta^2 + \zeta^{-2} + \zeta + \zeta^{-1} + 1 = 0 \end{aligned}$$

so α is a root of $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Z}[x]$. Since the degree of $f(x)$ is $\frac{1}{2}\phi(7) = 3$, this is the minimal polynomial of α . Allowing ζ to vary over the primitive seventh roots of unity in \mathbb{C} , we obtain the roots of $f(x)$ as

$$\alpha_k = e^{2k\pi i/7} + e^{-2k\pi i/7} = 2 \cos \frac{2k\pi}{7}, \quad k = 1, 2, 3.$$

The maximal real subfield of $\mathbb{Q}[\zeta]$ is $\mathbb{Q}[\alpha]$. Its ring of integers is

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3.$$

The values $\sin \frac{2k\pi}{7}$ are *not* algebraic integers for $k = 1, 2, 3$ (see Exercise #1); but their ratios are algebraic integers. For example,

$$\frac{\sin \frac{4\pi}{7}}{\sin \frac{6\pi}{7}} = \frac{(\zeta^2 - \zeta^{-2})/2i}{(\zeta^3 - \zeta^{-3})/2i} = \frac{\zeta^{-2}(\zeta^4 - 1)}{\zeta^{-3}(\zeta^6 - 1)} = \frac{1 - \zeta^4}{1 - \zeta^6} \zeta$$

which is a unit, by Theorem 4.3.

We come now to a very important characterization of roots of unity. Let $\zeta \in \mathbb{C}$ be a root of unity, so that $\zeta^n = 1$ for some positive integer n . Then ζ is an algebraic integer with $|\zeta| = 1$. But more than this, every algebraic conjugate of ζ is also a root of unity and so also has absolute value 1: that is, if σ is any field automorphism (of \mathbb{C} , or of $\mathbb{Q}[\zeta]$) then $|\sigma(\zeta)| = 1$. The following result shows that roots of unity are the *only* numbers with this property. Note that we strictly require algebraic integers here; for example $\frac{3}{5} + \frac{4}{5}i$ is an algebraic number, both of whose conjugates have absolute value 1; yet it is not a root of unity. Moreover, the algebraic integer $\alpha = \sqrt{-1 + \sqrt{2}} + i\sqrt{2 - \sqrt{2}}$ has $|\alpha| = 1$, yet it is not a root of unity. The minimal polynomial of α over \mathbb{Q} is $f(x) = x^8 + 12x^6 + 6x^4 + 12x^2 + 1$, which also has $\beta = (\sqrt{2 + \sqrt{2}} + \sqrt{1 + \sqrt{2}})i$ as a root. There exists $\sigma \in \text{Aut } \mathbb{C}$ (or $\sigma \in \text{Aut } E$ where E is the splitting field of $f(x)$) such that $\sigma(\alpha) = \beta$; and $|\beta| = \sqrt{2 + \sqrt{2}} + \sqrt{1 + \sqrt{2}} \neq 1$.

We denote by \mathbb{I} the ring of all algebraic integers in \mathbb{C} .

Theorem 4.10. Let $\alpha \in \mathbb{I}$. Then α is a root of unity iff every algebraic conjugate of α has absolute value 1.

Proof. (This argument is a fleshed-out version of [Wa, Lemma 1.6].) If α is a complex root of unity, say $\alpha^n = 1$, then all algebraic conjugates of α are also complex n -th roots of unity and they all have absolute value 1.

Conversely, suppose $\alpha \in \mathbb{I}$ has minimal polynomial $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in \mathbb{Z}[x]$ such that $|\alpha_1| = \cdots = |\alpha_n| = 1$. We may assume that $\alpha_1 = \alpha$. Let $K = \mathbb{Q}(\alpha)$, so that $[K : \mathbb{Q}] = n$; and consider the splitting field of $f(x)$, namely $E = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$, this being the Galois closure of K . The field E has $[E : \mathbb{Q}] = n[E : K]$ automorphisms, transitively permuting the n roots of $f(x)$. We now introduce a family of polynomials

$$g_r(x) = (x - \alpha_1^r)(x - \alpha_2^r) \cdots (x - \alpha_n^r) = \sum_{k=0}^n b_{r,k} x^{n-k}$$

indexed by $r = 1, 2, 3, \dots$. Each $b_{r,k}$ is a symmetric polynomial in $\alpha_1, \dots, \alpha_n$ (see Appendix A7) given by

$$b_{r,k} = (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \alpha_{i_1}^r \alpha_{i_2}^r \cdots \alpha_{i_k}^r;$$

in particular $b_{r,0} = 1$, $b_{r,1} = -\alpha_1^r - \alpha_2^r - \cdots - \alpha_n^r$, and $b_{r,n} = (-1)^n \alpha_1^r \alpha_2^r \cdots \alpha_n^r$. Since each $|\alpha_i| = 1$, we obtain the bounds

$$b_{r,0} = 1, \quad |b_{r,n}| = 1, \quad \text{and } |b_{r,k}| \leq \binom{n}{k} \text{ for each } k.$$

Each $\sigma \in \text{Aut } E$ permutes $\alpha_1, \dots, \alpha_n$ and so must satisfy $\sigma(b_{r,k}) = b_{r,k}$ for all r, k . By Galois theory, the fixed field of $\text{Aut } E$ is \mathbb{Q} ; but clearly each $b_{r,k}$ is an algebraic integer, so $b_{r,k} \in \mathbb{I} \cap \mathbb{Q} = \mathbb{Z}$ by Theorem A3.2(ii). Thus $g_r(x) \in \mathbb{Z}[x]$ for each $r \geq 1$. But there are only $2\binom{n}{k} + 1$ choices of integer $b_{r,k}$ satisfying the bounds indicated above for $k = 1, 2, \dots, n-1$ (also two choices of $b_{r,n} = \pm 1$, and the single choice $b_{r,0} = 1$), hence at most $N := 2 \prod_{k=1}^{n-1} [2\binom{n}{k} + 1]$ possibilities for each such polynomial $g_r(x)$. The set of all distinct roots of all the polynomials in our family $\{g_1(x), g_2(x), g_3(x), \dots\}$ is therefore a set of cardinality at most nN ; and all distinct powers α^r for $r \geq 1$ must lie in this finite set. Evidently the powers α^r cannot all be distinct, so α is a root of unity. \square

We can finally say something more about the group of units \mathcal{O}^\times of E . By Dirichlet's Theorem A3.6, $\mathcal{O}^\times \cong \{\text{roots of unity}\} \times \mathbb{Z}^{r+s-1}$ where E has r embeddings in \mathbb{R} and $2s$ pairs of complex conjugate embeddings in \mathbb{C} . By Theorem 4.2, we have a firm grasp on the first factor, consisting of the roots of unity (the torsion subgroup of \mathcal{O}^\times). For the second factor, the maximal free abelian subgroup of \mathcal{O} , note that $E := \mathbb{Q}[\zeta_n]$ has no embeddings in \mathbb{R} for $n > 2$; and it has $N := \frac{1}{2}\phi(n)$ pairs (under complex conjugation) of embeddings in \mathbb{C} . So $\mathcal{O}_E^\times \cong \langle \zeta_n \rangle \times \mathbb{Z}^{N-1}$, assuming $n > 2$ is even. Now the maximal real subfield $F := \mathbb{Q}[\alpha] \subset E$, $\alpha = \zeta + \zeta^{-1}$, has N real embeddings and no complex embeddings outside of \mathbb{R} . Its roots of unity are just ± 1 , so its group of units satisfies $\mathcal{O}_F^\times \cong \langle -1 \rangle \times \mathbb{Z}^{N-1}$. This means that the subgroup $\mathcal{O}_F^\times \subseteq \mathcal{O}_E^\times$ has finite index $[\mathcal{O}_E^\times : \mathcal{O}_F^\times] < \infty$. In other words, if we can identify the units in the maximal real subfield F , we shall have found 'almost all' the units in E .

A full enumeration of the unit group \mathcal{O}_E^\times is beyond the scope of this course; details can be found in [Wa, Chapter 8]. But for the important case of $n = p$ prime we have:

Theorem 4.11. Let $E = \mathbb{Q}[\zeta]$, $\zeta = \zeta_p$, p an odd prime; and let $F = \mathbb{Q}[\alpha]$ be its maximal real subfield, $\alpha = \zeta + \zeta^{-1}$. Then every unit $u \in \mathcal{O}_E^\times$ has the form $u = \zeta^r u_+$ for some $r \in \{0, 1, 2, \dots, p-1\}$ and some real unit $u_+ \in \mathcal{O}_F^\times$.

Proof. Since $u \in \mathcal{O}_E^\times$, we have $\bar{u} \in \mathcal{O}_E^\times$. Let $\beta = u/\bar{u}$, and note that $\beta \in \mathcal{O}_E^\times$. By Theorem 4.1,

$$|\sigma(\beta)|^2 = \sigma(\beta)\overline{\sigma(\beta)} = \sigma(\beta)\sigma(\bar{\beta}) = \sigma(\beta\bar{\beta}) = \sigma\left(\frac{u\bar{u}}{\bar{u}u}\right) = \sigma(1) = 1$$

for every $\sigma \in \text{Aut } E$, so $|\sigma(\beta)| = 1$. By Theorem 4.10, $\beta \in E$ is a root of unity. By Theorem 4.2, $\beta = \pm\zeta^k$ for some $k \in \mathbb{Z}$.

Suppose first that $\beta = -\zeta^k$. Recall from Theorem 4.4 that the element $\varepsilon = 1 - \zeta$ is irreducible of norm p . Clearly $\zeta \equiv 1 \pmod{(\varepsilon)}$. Expanding $u \in \mathcal{O}$ as $u = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2}$, it follows that $u \equiv a_0 + a_1 + a_2 + \cdots + a_{p-2} \pmod{(\varepsilon)}$ and $\bar{u} = a_0 + a_1\zeta^{p-1} + a_2\zeta^{p-2} + \cdots + a_{p-2}\zeta^2 \equiv a_0 + a_1 + a_2 + \cdots + a_{p-2} \equiv u \pmod{(\varepsilon)}$; so

$$2u = u - \zeta^k \bar{u} \equiv u - \bar{u} \equiv 0 \pmod{(\varepsilon)},$$

i.e. $2u = \varepsilon v$ for some $v \in \mathcal{O}_E$. But then taking norms, $2^{p-1} N_{E/\mathbb{Q}}(u) = p N_{E/\mathbb{Q}}(v)$ where all values of the norm are integers. But $N_{E/\mathbb{Q}}(u) = 1$ since u is a unit, so 2^{p-1} is divisible by p , a contradiction.

Thus $\beta = \zeta^k$ for some $k \in \mathbb{Z}/p\mathbb{Z}$. Since p is odd, we have $k = 2r$ for some $r \in \mathbb{Z}/p\mathbb{Z}$. Let $u_+ = \zeta^{-r}u$, so that u_+ is a unit. Also $u_+^2 = \zeta^{-2r}u^2 = \zeta^{-2r}u \cdot \bar{u}\zeta^k = u\bar{u} = |u|^2$, which is a positive real number; so $u_+ \in \mathbb{R}$. This means that $u_+ \in E \cap \mathbb{R} = F$, the maximal real subfield of E . Moreover, $u = \zeta^r u_+$ as required. \square

Of course, we will not find these observations to be of much use in identifying the group of units of E , unless we can first find the group of units of F . Fortunately, however, the units of Theorem 4.3 are sufficient to generate almost the full group of units (meaning a subgroup of finite index in the full group of units). Although the ratios $\frac{1-\zeta^r}{1-\zeta^s}$ are not generally real, they do provide generators of \mathcal{O}_F^\times after factoring out roots of unity; see Example 4.9. More explicitly, let $n > 2$, and for convenience denote by ζ_{2n} a primitive $2n$ -th root of unity satisfying $\zeta_{2n}^2 = \zeta_n$. Also let r, s be integers relatively prime to n . Then Theorem 4.3 gives us units in E of the form

$$\frac{1 - \zeta_n^r}{1 - \zeta_n^s} = \frac{1 - \zeta_{2n}^{2r}}{1 - \zeta_{2n}^{2s}} = \frac{\zeta_{2n}^r (\zeta_{2n}^{2r} - \zeta_{2n}^{-2r})}{\zeta_{2n}^s (\zeta_{2n}^{2s} - \zeta_{2n}^{-2s})} = \zeta_{2n}^{r-s} \frac{\sin \frac{2r\pi}{2n}}{\sin \frac{2s\pi}{2n}} = \zeta_n^{\frac{r-s}{2}} \frac{\sin \frac{r\pi}{n}}{\sin \frac{s\pi}{n}} \in \mathcal{O}_E^\times,$$

whence also real units $\frac{\sin(r\pi/n)}{\sin(s\pi/n)} \in \mathcal{O}_F^\times$. Note here that if n is even, then both r and s are odd (as they are relatively prime to n), so the exponent $\frac{r-s}{2}$ is an integer; whereas if n is odd, then 2 is invertible mod n so $\frac{r-s}{2}$ is again well-defined in $\mathbb{Z}/n\mathbb{Z}$. Now if we fix s (e.g. $s = 1$) and vary r over the remaining $N - 1$ choices of integers $< \frac{n}{2}$ relatively prime to n , we obtain generators for a large subgroup of \mathcal{O}_F^\times . (As usual, ‘large’ means having finite index in the full group of real units \mathcal{O}_F^\times .)

At this point, we must disclose two difficulties: one of a mathematical nature, and the other strictly terminological. The units constructed above do not suffice to generate the full group of units. The term ‘**cyclotomic unit**’, which arguably should refer to a unit in the cyclotomic field (just as one speaks of a cyclotomic number, cyclotomic integer, etc. for elements of $\mathbb{Q}[\zeta]$, $\mathbb{Z}[\zeta]$, and related concepts that we have not mentioned in these notes) has instead come to mean one of the units specifically of the form $\frac{1-\zeta^r}{1-\zeta^s}$ in E , or of

the form $\frac{\sin(r\pi/n)}{\sin(s\pi/n)}$ in F . Determining the (finite) index of the subgroup of \mathcal{O}^\times generated by these ‘cyclotomic units’ in either case, is a difficult computational problem in general, and is in fact related to the problem of computing class numbers. Computational software gives us the answer for specific values of n of modest size; but general formulas tend to rely on analytic methods for which computations can require great numerical finesse.

Before closing this Section, we briefly discuss factorization in $E = \mathbb{Q}[\zeta_n]$. The fields $\mathbb{Q}[\zeta_n]$ have unique factorization for $n \leq 22$ and for finitely many larger values of n ; see [Wa, Chapter 11]. The primes p for which $\mathbb{Q}[\zeta_p]$ has unique factorization, are known to be exactly the primes $p \leq 19$. Uniqueness of factorization for $n = 3, 4$ is easily shown using the Euclidean property; see Corollary A3.16.

Example 4.12: $\mathbb{Q}[\zeta_{23}]$ is neither a PID nor a UFD. The field $E = \mathbb{Q}[\zeta_{23}]$ does not have unique factorization. To see this, by Theorem A3.14 it suffices to find an ideal in $\mathcal{O}_E = \mathbb{Z}[\zeta]$, $\zeta = \zeta_{23}$, which is not principal. First note that $\sqrt{-23} \in E$, which follows from Theorem 10.13. The subfield $F = \mathbb{Q}[\sqrt{-23}] \subset E$ has as its ring of integers $\mathcal{O}_F = \mathbb{Z}[\theta]$, $\theta = \frac{1}{2}(1 + \sqrt{-23})$ by Example A3.5. Consider the ideals $\mathfrak{p} = (2, \theta) \subset \mathcal{O}_F$ (note: $\mathfrak{p} = 2\mathcal{O}_F + \theta\mathcal{O}_F$) and $\bar{\mathfrak{p}} = (2, \bar{\theta})$. We have $2 = (-2)2 + \theta\bar{\theta} \in \mathfrak{p}\bar{\mathfrak{p}}$, and the reverse containment follows from $(2a+b\theta)(2c+d\bar{\theta}) = 2(2ac+ad\bar{\theta}+bc\theta+3bd) \in (2)$. Thus $(2) = \mathfrak{p}\bar{\mathfrak{p}}$. Now the norm map on \mathcal{O}_F is defined by $N(a+b\theta) = (a+b\theta)(a+b\bar{\theta}) = a^2 + ab + 6b^2$. In particular, $N(\mathfrak{p})N(\bar{\mathfrak{p}}) = N(2) = 4$ and since $N(\bar{\mathfrak{p}}) = N(\mathfrak{p})$ by algebraic conjugation, we must have $N(\mathfrak{p}) = N(\bar{\mathfrak{p}}) = 2$. Evidently the ideals \mathfrak{p} and $\bar{\mathfrak{p}}$ are nonprincipal; for example if $\mathfrak{p} = (a+b\theta)$, $a, b \in \mathbb{Z}$, then $a^2 + ab + 6b^2 = N(\mathfrak{p}) = 2$; but this has no solution in integers. (If $2 = a^2 + ab + 6b^2 = (a + \frac{b}{2})^2 + \frac{23}{4}b^2 \geq \frac{23}{4}b^2$, then we must have $b = 0$; but then $a^2 = 2$, a contradiction.) Now the extension $E \supset F$ is Galois of degree $\frac{1}{2}\phi(23) = 11$, with Galois group $G = G(E/F) = \{\iota, \sigma, \sigma^2, \dots, \sigma^{10}\}$. The ideal $\mathfrak{p}\mathcal{O}_E \subset \mathcal{O}_E$ has prime factorization of the form either

- (i) $\mathfrak{p}\mathcal{O}_E = \mathfrak{P}$ prime, $N_{E/F}(\mathfrak{P}) = 2^{11}$, $\sigma(\mathfrak{P}) = \mathfrak{P}$; or
- (ii) $\mathfrak{p}\mathcal{O}_E = \mathfrak{P}\sigma(\mathfrak{P})\sigma^2(\mathfrak{P}) \cdots \sigma^{10}(\mathfrak{P})$, $N_{E/F}(\sigma^i(\mathfrak{P})) = 2$. We do not require (or assume) that the eleven prime factors are distinct.

Suppose that $\mathfrak{P} = \pi\mathcal{O}_E$ is principal. In case (i) this yields $\pi \in F$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F = \pi\mathcal{O}_F$, a principal ideal in \mathcal{O}_F , a contradiction. In case (ii),

$$\mathfrak{p}\mathcal{O}_E = \prod_{i=0}^{10} \sigma^i(\mathfrak{P}) = \left(\prod_{i=0}^{10} \sigma^i(\pi) \right) \mathcal{O}_E = N_{E/F}(\pi) \mathcal{O}_E$$

where $N_{E/F}(\pi) \in F$; but then $\mathfrak{p} = N_{E/F}(\pi)\mathcal{O}_E \cap \mathcal{O}_F = N_{E/F}(\pi)\mathcal{O}_F$ is principal, a contradiction.

Exercises 4.

1. Let $\zeta = \zeta_{2n}$, $n \geq 3$.
 - (a) Using the relation $2i \sin \frac{k\pi}{n} = \zeta^k - \zeta^{-k} = \zeta^k(1 - \zeta^{-2k})$, show that $\prod_{k=1}^{n-1} \sin \frac{k\pi}{n} = \frac{n}{2^{n-1}}$.
 - (b) Use (a) to show that $\sin \frac{k\pi}{n}$ cannot always be an algebraic integer.
 - (c) Show that *none* of the values $\sin \frac{k\pi}{7}$, $k = 1, 2, \dots, 6$, are algebraic integers.
2. In the notation of Example 4.12, consider the nonprincipal prime ideal $\mathfrak{p} = (2, \theta) \subset \mathcal{O}_F$. Show that $\mathfrak{p}^3 \subset \mathcal{O}_F$ is principal. (*Hint:* Verify that $2 - \theta = 2^3 + 2^2\theta + \theta^3 \in \mathfrak{p}^3$. Argue that $(2 - \theta) \subseteq \mathfrak{p}^3$; then compare norms on both sides to obtain equality.)
3. Recall that $1 - \zeta_p \in \mathbb{Z}[\zeta_p]$ is irreducible for p prime (Theorem 4.4). The condition that p is prime is strictly necessary here. Show, for example, that if $\zeta = \zeta_{15}$, then $1 - \zeta$ is a unit in $\mathbb{Z}[\zeta]$. State and prove a generalization of this fact.

5. Fermat's Last Theorem

Fermat's Last Theorem (FLT) is, of course, the statement that the equation $x^n + y^n = z^n$ has no positive integer solutions for exponent $n > 2$. While interest in FLT has had a profound impact on modern mathematics, we shall have nothing to say here about the recognized proof of this theorem due to Wiles and others, since this involves a great many topics beyond the scope of our course. Our purpose is rather to say something about the role of cyclotomic fields in the earliest work on FLT. One might justifiably say that the early development of the theory of cyclotomic fields was largely motivated by FLT; but by the time we came to accept that other tools would be required to resolve FLT, the theory and applications of cyclotomic fields have grown far beyond their original confines.

The role of cyclotomic fields in studying FLT is evident already in the smallest case $n = 3$. Fermat claimed to have settled this case in his correspondence, although there is no surviving copy of his proof. We presume it was along the lines of Euler's later proof of 1770, which is essentially the proof we give below. There is a surviving copy of Fermat's proof for the exponent $n = 4$, also using his 'method of infinite descent'. While the case $n = 3$ is a little more involved, the case of prime exponent is more typical in its of cyclotomic fields; so it is this case we have chosen to highlight here.

Theorem 5.1. The equation $x^3 + y^3 = z^3$ has no solution in positive integers.

Proof. After replacing the integer z by $-z$, the equation to be solved takes the more symmetrical form $x^3 + y^3 + z^3 = 0$; here we may suppose there is a solution in nonzero integers, and seek a contradiction. But it will be easier to prove a seemingly stronger statement. Let $\mathcal{O} = \mathbb{Z}[\omega]$, the ring of Eisenstein integers, where $\omega = \zeta_3$. The ring \mathcal{O} is a UFD; see Corollary A3.16. Its group of units is the finite group of sixth roots of unity $\mathcal{O}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$; see Example A3.8. Now we suppose that

$$(5.2) \quad x^3 + y^3 + uz^3 = 0 \text{ for some nonzero } x, y, z \in \mathcal{O} \text{ and } u \in \mathcal{O}^\times;$$

and we seek a contradiction. The contradiction to which we are led, is that any solution of (5.2) leads to a smaller solution of (5.2) (this is Fermat's 'method of descent'). Here 'smaller' is in terms of the norms; and since (absolute values of) norms lie in \mathbb{N} , this leads to an infinite descending sequence in \mathbb{N} , hence a contradiction. The advantage of (5.2) over the original equation, is that at the descent step, we have a stronger inductive hypothesis available (as well as a stronger conclusion to fulfill). Put another way, we may further suppose that our solution of (5.2) is as small as possible, and obtain from this an outright contradiction. In particular,

$$(5.3) \quad \text{no irreducible element } \pi \in \mathcal{O} \text{ divides any two of } x, y, z;$$

otherwise π divides the third member of the triple and then dividing by the common factor π , we would obtain a smaller nonzero solution of (5.2).

A typical element $z = a + b\omega \in \mathcal{O}$ ($a, b \in \mathbb{Z}$) has norm $N(z) = z\bar{z} = a^2 - ab + b^2$. The irreducible element $\varepsilon = 1 - \omega$ has norm $N(\varepsilon) = 3$; and the rational prime 3 ramifies in \mathcal{O} as $(3) = (\varepsilon)^2$ (see Theorem 4.4). Indeed, $\varepsilon^2 = 1 - 2\omega + \omega^2 = -3\omega$ and $(\varepsilon^2) = (3)$ since $-\omega$ is a unit.

Now it is profitable to consider possibilities for each of the variables $x, y, z \pmod{\varepsilon}$. We have $\mathcal{O}/(\varepsilon) \cong \mathbb{F}_3$. This follows directly from the formula $N((\varepsilon)) = |N(\varepsilon)| = 3$; but one can also note that every $x \in \mathcal{O}$ can be expressed uniquely as $x = a + b\varepsilon$; so $x \equiv a \pmod{\varepsilon}$, 1 or $2 \pmod{\varepsilon}$ (recall that $3 \equiv 0 \pmod{\varepsilon}$). If $x = 1 + b\varepsilon$ then

$$x^3 = 1 + 3b\varepsilon + 3b^2\varepsilon^2 + \varepsilon^3 = 1 - 3(b^3 - b)\varepsilon - 9b^2(b+1)\omega \equiv 1 \pmod{9}$$

since $b^3 - b = (b-1)b(b+1) \equiv 0 \pmod{3}$ (this being a product of three consecutive integers). Replacing x by $-x$ shows that $x^3 \equiv -1 \pmod{9}$ also whenever $x \equiv -1 \pmod{\varepsilon}$. The third case $x \equiv 0 \pmod{\varepsilon}$ is even easier. Thus

$$(5.4) \quad \text{for } x \in \mathcal{O}, \text{ we have } x^3 \equiv \begin{Bmatrix} 1 \\ 0 \\ -1 \end{Bmatrix} \pmod{9} \text{ according as } x \equiv \begin{Bmatrix} 1 \\ 0 \\ -1 \end{Bmatrix} \pmod{\varepsilon}.$$

Now consider (5.2) $\pmod{9}$ and apply (5.4) to see that x, y, z must be congruent to $0, 1, -1 \pmod{\varepsilon}$ (in some order). Moreover if $z \equiv \pm 1 \pmod{\varepsilon}$ then we must have $u = \pm 1$; but in this case we may exchange z with either x or y to get $x \equiv 1 \pmod{\varepsilon}$, $y \equiv -1 \pmod{\varepsilon}$, $z \equiv 0 \pmod{\varepsilon}$. Now (5.4) gives $x^3 + y^3 \equiv 0 \pmod{9}$, so $z^3 \equiv 0 \pmod{9}$, i.e. $z^3 \equiv 0 \pmod{\varepsilon^4}$. Thus

$$(5.5) \quad x \equiv 1 \pmod{\varepsilon}; \quad y \equiv -1 \pmod{\varepsilon}; \quad z \equiv 0 \pmod{\varepsilon^2}. \quad \text{We may write } z = \varepsilon^k z' \text{ where } k \geq 2 \text{ and } z' \in \mathcal{O}, z' \not\equiv 0 \pmod{\varepsilon}.$$

Now compare irreducible factors on both sides of

$$(5.6) \quad (x + y)(x + \omega y)(x + \omega^2 y) = -u\varepsilon^{3k}(z')^3.$$

If an irreducible $\pi \in \mathcal{O}$ divides both $x + y$ and $x + \omega y$, then it divides their difference which is $(1 - \omega)y = \varepsilon y$. However, π cannot divide y ; otherwise π also divides x , contrary to (5.3). The same argument, applied to the other parenthetical factors on the left side of (5.6), shows that the gcd of any two of these factors is either 1 or ε . But $x + \omega^j y \equiv x + y \equiv 1 - 1 \equiv 0 \pmod{\varepsilon}$ for all $j \in \{0, 1, 2\}$. It follows that

$$(5.7) \quad \text{the factors } x+y, x+\omega y, x+\omega^2 y \text{ are, in some order, equal to } u_1\varepsilon\alpha_1^3, u_2\varepsilon\alpha_2^3 \text{ and } u_3\varepsilon^{3k-2}\alpha_3^3 \text{ where } u_i \in \mathcal{O}^\times \text{ and } \alpha_i \in \mathcal{O} \text{ are not divisible by } \varepsilon.$$

Without loss of generality, it is the third factor $x + \omega^2 y$ that is divisible by ε^{3k-2} ; otherwise replace y by $\omega^j y$ for some j , thereby cycling the three factors while preserving the

conditions (5.5). Now $u_i \in \{\pm 1, \pm \omega, \pm \omega^2\}$; but without loss of generality, $u_i \in \langle \omega \rangle$, since any ‘-’ signs can be absorbed into α_i . Therefore we may assume

$$(5.8) \quad x + y = \omega^{j_1} \varepsilon \alpha_1^3, \quad x + \omega y = \omega^{j_2} \varepsilon \alpha_2^3, \quad x + \omega^2 y = \omega^{j_3} \varepsilon^{3k-2} \alpha_3^3.$$

Adding the three expressions in (5.8) gives

$$\begin{aligned} -\omega^2 \varepsilon^2 x = 3x &= \omega^{j_1} \varepsilon \alpha_1^3 + \omega^{j_2} \varepsilon \alpha_2^3 + \omega^{j_3} \varepsilon^{3k-2} \alpha_3^3; \\ -\omega^2 \varepsilon x &= \omega^{j_1} \alpha_1^3 + \omega^{j_2} \alpha_2^3 + \omega^{j_3} \varepsilon^{3k-3} \alpha_3^3. \end{aligned}$$

Since $k \geq 2$, $x \equiv 1 \pmod{\varepsilon}$ and $\omega^j \equiv 1 - j\varepsilon \pmod{3}$, this gives

$$-\varepsilon \equiv (1 - j_1 \varepsilon) \alpha_1^3 + (1 - j_2 \varepsilon) \alpha_2^3 \pmod{3}$$

and since $\alpha_i \equiv \pm 1 \pmod{\varepsilon}$, (5.4) gives $\alpha_i^3 \equiv \pm 1 \pmod{9}$. Evidently $\alpha_1^3 \equiv 1$ and $\alpha_2^3 \equiv -1 \pmod{9}$ (or we reverse the roles of α_1 and α_2 so that this is the case) and $j_2 \equiv j_1 - 1 \pmod{3}$. Now

$$0 = (x + y) + \omega(x + \omega y) + \omega^2(x + \omega^2 y) = \omega^{j_1} \varepsilon \alpha_1^3 + \omega^{j_2+1} \varepsilon \alpha_2^3 + \omega^{j_3+2} \varepsilon^{3k-2} \alpha_3^3$$

and so

$$(5.9) \quad 0 = \alpha_1^3 + \alpha_2^3 + \omega^{j_3-j_1+2} (\varepsilon^{k-1} \alpha_3)^3.$$

Thus $(\alpha_1, \alpha_2, \varepsilon^{k-1} \alpha_3)$ solves the same equation as (x, y, z) in (5.2). By the remarks following (5.2), it suffices to show that the new solution is smaller in the sense of norm, than the original solution; specifically, we show that

$$(5.10) \quad 0 < |\mathbf{N}(\alpha_1 \alpha_2 \varepsilon^{k-1} \alpha_3)| < |\mathbf{N}(xyz)|.$$

To prove (5.10), observe that

$$\begin{aligned} -uz^3 = x^3 + y^3 &= (x + y)(x + \omega y)(x + \omega^2 y) = (\omega^{j_1} \varepsilon \alpha_1^3)(\omega^{j_2} \varepsilon \alpha_2^3)(\omega^{j_3} \varepsilon^{3k-2} \alpha_3^3) \\ &= \omega^{j_1+j_2+j_3} \varepsilon^3 (\alpha_1 \alpha_2 \varepsilon^{k-1} \alpha_3)^3. \end{aligned}$$

Taking norms of both sides in the extension $\mathbb{Q}[\omega] \supset \mathbb{Q}$ gives $\mathbf{N}(z)^3 = \pm 27 \mathbf{N}(\alpha_1 \alpha_2 \varepsilon^{k-1} \alpha_3)^3$ and so

$$0 < 3|\mathbf{N}(\alpha_1 \alpha_2 \varepsilon^{k-1} \alpha_3)| = |\mathbf{N}(z)| \leq |\mathbf{N}(xyz)|$$

and (5.10) follows, completing the proof of Theorem 5.1. \square

Now consider the general case of FLT. Because Fermat himself proved his conjecture for $n = 4$, clearly we can confine our attention to the case of prime exponent $p \geq 3$. So

in the following, we assume p is an odd prime; and we further suppose $x^p + y^p = z^p$ with x, y, z positive integers, hoping to obtain thereby a contradiction.

We can assume any two of x, y, z are relatively prime; otherwise all three have a common factor which can then be divided out to obtain a smaller solution in positive integers. Next, one observes that in $\mathbb{Z}[\zeta_p]$ we have the factorization

$$(5.11) \quad x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y) = z^p.$$

This relation clearly begs us to compare prime factors on both sides, expecting to find that apart from units and powers of $\varepsilon = 1 - \zeta$, the factors $x + \zeta^i y$ are pairwise relatively prime p th powers. This is the key idea in the proof of Theorem 1.1; and it figures prominently also for the classification of primitive Pythagorean triples (the case of exponent $n = 2$). This plan, despite its merits, runs into difficulty in $\mathbb{Z}[\zeta_p]$, where unique factorization does not hold in general. Some famous early attempts to prove FLT (including some by the best mathematicians of the 19th century) foundered precisely by assuming $\mathbb{Q}[\zeta]$ to be a UFD in general. It is natural to speculate that Fermat himself fell prey to this fallacy, although presumably we will never know this. It was largely to repair this defect that the concept of ‘ideal’ was introduced (so named by Ernst Kummer whose work on cyclotomic fields, together with Sophie Germain’s contributions, led the progress toward FLT during the 19th century).

Experience has also shown that it is profitable to approach (5.11) in two separate cases: (i) none of x, y, z are divisible by p ; or (ii) exactly one of x, y, z is divisible by p . Tradition refers to these two cases as the **first case** and the **second case** of FLT. The following result concerns the first case; for the counterpart of this result in the second case, also using the theory of cyclotomic fields, see [Wa, Chapter 9]. Refer to Appendix A3 regarding the class number of an extension.

Theorem 5.12. Suppose that $p > 2$ is a prime for which the class number of $\mathbb{Z}[\zeta]$, $\zeta = \zeta_p$, is not divisible by p . Then the equation $x^p + y^p = z^p$ has no solution in integers x, y, z relatively prime to p .

Proof. The cases $p = 3, 5$ are easily disposed of, even without Theorem 1.1. For $p = 3$, we have $z^3 \equiv \pm 1 \pmod{9}$ whenever $\gcd(z, 3) = 1$; and by this same fact, $x^3 + y^3 \equiv 0$ or $\pm 2 \pmod{9}$. So there are no solutions for $p = 3$ in the first case. Exactly the same reasoning works for $p = 5$, by considering Fermat’s equation mod 25. Thus we may assume $p \geq 7$. Let $\mathcal{O} = \mathbb{Z}[\zeta]$, $\zeta = \zeta_p$. Recall that the element $\varepsilon = 1 - \zeta \in \mathcal{O}$ is irreducible and $\mathbb{Z} \cap \varepsilon \mathcal{O} = p\mathbb{Z}$; see Theorem 4.4.

We claim that the ideals $(x + \zeta^i y) \subseteq \mathcal{O}$ are pairwise relatively prime for $i = 0, 1, 2, \dots, p-1$. Suppose that on the contrary, $(x + \zeta^i y)$ and $(x + \zeta^j y)$ have a common prime factor $\mathfrak{P} \subset \mathcal{O} = \mathbb{Z}[\zeta]$, $0 \leq i < j < p$. Then $(1 - \zeta^{j-i})y = \zeta^{-i}[(x + \zeta^i y) - (x + \zeta^j y)] \in \mathfrak{P}$; so by

Theorem 4.3, either $\mathfrak{P} = (1-\zeta) = (\varepsilon)$ or $y \in \mathfrak{P}$. Similarly, $(1-\zeta^{j-i})x = (x+\zeta^j y) - \zeta^{j-i}(x+\zeta^i y) \in \mathfrak{P}$, so either $\mathfrak{P} = (\varepsilon)$ or $x \in \mathfrak{P}$. We cannot have both x and y in \mathfrak{P} , otherwise x, y are both divisible by the prime p' satisfying $p'\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$. Thus $\mathfrak{P} = (\varepsilon)$ and z^n is divisible by $(x+\zeta^i y) - (x+\zeta^j y) = \zeta^i(1-\zeta^{j-i})y$ which means that $p \mid z$. This violates the assumption that we are in the ‘first case’ of FLT. This proves our initial claim.

By considering prime ideal factors on both sides of (5.11), it follows easily that each ideal $(x+\zeta^i y)$ is itself the p -th power of an ideal: $(x+\zeta^i y) = \mathcal{B}_i^p$ for some ideal $\mathcal{B}_i \subseteq \mathcal{O}$. Let h be the class number of \mathcal{O} ; so we have a principal ideal $\mathcal{B}_i^h = (a_i)$ for some $a_i \in \mathcal{O}$. By hypothesis there exists a positive integers k, ℓ such that $mp = kh + 1$, so $(x+\zeta^i y)^m = \mathcal{B}_i^{mp} = \mathcal{B}_i^{kh+1} = (\beta_i)^k \mathcal{B}_i$. This implies that the ideal $\mathcal{B}_i \subseteq \mathcal{O}$ is principal: $\mathcal{B}_i = (\beta_i)$, $\beta_i \in \mathcal{O}$.

Now abbreviate $\mathcal{B} = \mathcal{B}_1$, $\beta = \beta_1$. We have $(x+\zeta y) = \mathcal{B}^p = (\beta)^p$; so by Theorem 4.11, we have $x+\zeta y = \zeta^k u \beta^p$ for some $k \in \{0, 1, 2, \dots, p-1\}$ and a real unit $u \in \mathbb{Z}[\zeta+\zeta^{-1}]$. Also writing $\beta = \sum_{i=0}^{p-2} b_i \zeta^i$, where $b_i \in \mathbb{Z}$, we have $\beta^p \equiv \sum_{i=0}^{p-2} (b_i \zeta^i)^p \equiv \sum_{i=0}^{p-2} b_i^p \equiv b \pmod{p}$ for some $b \in \mathbb{Z}$. Thus $x+\zeta y \equiv \zeta^k u b \pmod{p}$; and after complex conjugation, $x+\zeta^{-1} y \equiv \zeta^{-k} u b \pmod{p}$. Since u is a unit and b an integer, we get

$$(5.13) \quad x + \zeta y - \zeta^{2k} x - \zeta^{2k-1} y = (x + \zeta y) - \zeta^{-2k} (x + \zeta^{-1} y) \in p\mathcal{O}.$$

If the powers $1, \zeta, \zeta^{2k}, \zeta^{2k-1}$ are distinct, (5.13) gives a contradiction, as we now show. Any $p-1$ of the distinct powers $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ form a basis for $\mathbb{Q}[\zeta]$ over \mathbb{Q} . Since $p \geq 7$ (the case to which we reduced at the outset), we may choose such a basis containing $1, \zeta, \zeta^{2k}, \zeta^{2k-1}$. Here we assume for the sake of argument that $1, \zeta, \zeta^{2k}, \zeta^{2k-1}$ are distinct members of $\{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$; and if this is not the case, the choice of basis can be adapted accordingly. Then by (5.13) we have

$$x + \zeta y - \zeta^{2k} x - \zeta^{2k-1} y = p(a_0 + a_1 \zeta + a_2 \zeta^2 + \dots + a_{p-2} \zeta^{p-2})$$

for some $a_0, a_1, a_2, \dots, a_{p-2} \in \mathbb{Z}$. This gives $x, y \in p\mathbb{Z}$, contrary to hypothesis.

Now we deal with the few special cases not covered by the previous argument. Since $\zeta \neq 1$ and $\zeta^{2k} \neq \zeta^{2k-1}$, these are the cases

- (i) $\zeta^{2k} = 1$. In this case, (5.13) reduces to $\zeta^{-1}(\zeta^2 - 1)y \in p\mathcal{O}$. By Theorem 4.4 and the fact that $p > 2$, this gives $y \in p\mathbb{Z}$, contrary to hypothesis.
- (ii) $\zeta = \zeta^{2k-1}$. Here, (5.13) becomes $(1 - \zeta^2)x \in p\mathcal{O}$, leading to a contradiction as in (i).
- (iii) $\zeta^{2k-1} = 1$. Here, (5.13) becomes $(1 - \zeta)(x - y) \in p\mathcal{O}$, yielding $x \equiv y \pmod{p}$. We may assume however that this congruence does not hold. If one replaces z by $-z$, then Fermat's equation takes the more symmetrical form $x^p + y^p + z^p = 0$; and we are required to prove that this equation has no solution in integers relatively prime to p . Under these hypotheses, however, x, y, z cannot all be congruent mod p , as this would entail $3x^p \equiv 0 \pmod{p}$, which cannot hold for $p > 3$ and $p \nmid x$. By symmetry, we

may therefore assume $x \not\equiv y \pmod{p}$ and move the third variable z to the right side of Fermat's equation.

This completes the proof of Theorem 5.12. \square

A prime p is called **regular** if the class number of $\mathbb{Z}[\zeta_p]$ is not divisible by p ; otherwise p is **irregular**. The first few irregular primes are 37, 59, 67, 101, 103, etc.; these are the primes for which the hypotheses of Theorem 5.12 fail. Reasonable heuristics, backed by computational evidence, support the conjecture that a proportion $e^{-1/2} \approx 61\%$ of primes are regular; so it might seem that the theory of cyclotomic fields solves FLT for 'most' prime exponents. However, it is *not known* that there are infinitely many regular primes. (Curiously, the set of irregular primes *is* known to be infinite, despite being apparently less dense than the sequence of regular primes.) Fortunately there is a test for regularity of primes which is (at least conceptually) rather explicit.

The sequence of **Bernoulli numbers** $B_0, B_1, B_2, B_3, \dots$ given by

$$1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, -\frac{1}{42}, \dots$$

may be defined via the Taylor series expansion

$$\begin{aligned} \frac{x}{e^x - 1} &= \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n \\ &= 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 + \frac{1}{30240}x^6 - \frac{1}{1209600}x^8 + \frac{1}{47900160}x^{10} - \frac{691}{1307674368000}x^{12} \\ &\quad + \frac{1}{74724249600}x^{14} - \frac{3617}{10670622842880000}x^{16} + \frac{43867}{5109094217170944000}x^{18} - \dots \end{aligned}$$

It is easily shown that $B_n = 0$ for even integers $n \geq 4$; and that the nonzero Bernoulli numbers alternate in sign. Among the many uses of Bernoulli numbers, we mention

- (i) an exact formula for certain special values of the Riemann zeta function:

$$\zeta(2k) = (-1)^{k+1} \frac{2^{2k-1} \pi^{2k}}{(2k)!} B_{2k}, \quad k = 1, 2, 3, \dots;$$

- (ii) a formula expressing the sum of the k th powers of the first n positive integer as a polynomial in n of degree $k+1$:

$$1^k + 2^k + 3^k + \dots + n^k = \frac{1}{k+1} \sum_{i=0}^k (-1)^i \binom{k+1}{i} B_i n^{k+1-i}.$$

In the current context, the relevance of the Bernoulli numbers is that

- (5.14) a prime p is regular iff none of the Bernoulli numbers B_k , for $k = 2, 4, 6, \dots, p-3$, have numerator divisible by p (when expressed as reduced fractions).

For example, 691, 3617 and 43867 (which are primes) must be irregular; and the first irregular prime, 37, divides the numerator of

$$B_{32} = -\frac{7709321041217}{510} = -\frac{37 \cdot 683 \cdot 305065927}{2 \cdot 3 \cdot 5 \cdot 17}.$$

Exercises 5.

1. Find a positive integer n for which the ring of cyclotomic integers $\mathbb{Z}[\zeta_n]$ contains nonzero solutions of $x^3 + y^3 = z^3$.

We say that p **sharply divides** n , denoted $p \parallel n$, if p divides n , but p^2 does not divide n .

2. Let p be an odd prime, and let x and y be relatively prime nonzero integers with $x + y \neq 0$.

(a) Show that $\gcd(x + y, (x^p + y^p)/(x + y)) = 1$ or p .

(b) If p divides $x + y$, show that p also divides $x^p + y^p$ and p sharply divides $(x^p + y^p)/(x + y)$.

Hint: Let $u = x + y$. Simplify the expression $((u - y)^p + y^p)/u$ after first expanding $(u - y)^p$ by the Binomial Theorem. At some point you may also want to recall Fermat's Little Theorem.

3. Let p be an odd prime; and let x, y, z be pairwise relatively prime nonzero integers satisfying $x^p + y^p + z^p = 0$. Recall that p divides at most one of x, y, z .

(a) If $p \nmid z$, show that $x + y = a^p$ and $(x^p + y^p)/(x + y) = A^p$ for some integers a, A . (*Hint:* Use #2.)

(b) In the first case of FLT, $p \nmid xyz$. Argue as in (a) to obtain $x + z = b^p$, $y + z = c^p$ and $2x = a^p + b^p - c^p$.

(c) If $p \mid z$ then we are in the second case of FLT, and (a) fails. Show that in this case, we instead obtain $x + y = p^{p-1}a^p$ and $(x^p + y^p)/(x + y) = pA^p$ for some integers a, A .

A pair of odd primes $\{p, q\}$ such that $q = 2p + 1$ is a **Sophie Germain pair of primes**. It is conjectured that there are infinitely many such pairs of primes.

4. Suppose we have a pair of Sophie Germain primes $\{p, q\}$, $q = 2p + 1$. As in the first case of FLT, suppose that x, y, z are pairwise relatively prime integers satisfying $x^p + y^p + z^p = 0$ with $p \nmid xyz$.

(a) If $q \nmid x$, show that $x^p \equiv \pm 1 \pmod{q}$. *Hint:* Theorem 3.4.

(b) Show that $q \mid xyz$. Hence without loss of generality, we assume $q \mid x$.

(c) Show that $q \mid abc$ where a, b, c are as in #3.

(d) By considering in cases $q \mid a$, $q \mid b$ or $q \mid c$, obtain a contradiction.

This solved the first case of FLT for many primes, and conjecturally an infinite class of primes. This breakthrough of Sophie Germain was later generalized by Legendre, enabling all prime $p < 100$ to be dealt with. Subsequent work of others in the 20th century, all based on Sophie Germain's idea, was able to prove the first case of FLT for an infinite class of primes (yet without proving there are infinitely many Sophie Germain primes).

6. Characters of Finite Abelian Groups

Let G be a finite abelian group of order n . Here we consider G to be multiplicative, as we are free to do, up to isomorphism. (The difficulty with additive groups is a purely

notational issue that arises when describing group rings. In Section 7, where we focus on group rings, we will discuss the natural accommodations for dealing with additive groups; but for now, there is no need to be distracted by this.) A **character** of G is a homomorphism $\chi : G \rightarrow \mathbb{C}^\times$; thus $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in G$. (So χ is what would be called a **linear character** in the larger world of group theory.) Since $x^n = 1$ for all $x \in G$ (this being a special case of Lagrange's Theorem), $\chi(x)^n = \chi(x^n) = \chi(1) = 1$ and so all values of χ are complex roots of unity. In fact, all values of χ are complex m -th roots of unity, where m is the **exponent** of G (this being the smallest positive integer m such that $x^m = 1$ for all $x \in G$). Note the exponent m of G divides $n = |G|$; and $m = n$ iff G is cyclic.

If $\chi, \chi' : G \rightarrow \mathbb{C}^\times$ are characters, then the product $\chi\chi' : G \rightarrow \mathbb{C}^\times$ defined pointwise by $(\chi\chi')(x) = \chi(x)\chi'(x)$ is clearly a character. The **trivial character** (or **principal character**) is the constant map $G \rightarrow \{1\} \subset \mathbb{C}^\times$. The multiplicative inverse of a character χ is its complex conjugate $\bar{\chi}(x) = \chi(x)^{-1}$ (since the multiplicative inverse of every complex root of unity is its complex conjugate). We see that the set of characters of G forms a multiplicative group, which we call the **dual group** \widehat{G} .

Theorem 6.1. Let G, G_1, G_2 be finite abelian groups. Then

- (a) $\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$, and
- (b) $\widehat{\widehat{G}} \cong G$.

Proof. (a) Every ordered pair $(\chi_1, \chi_2) \in \widehat{G_1} \times \widehat{G_2}$ defines a map

$$\chi_1 \times \chi_2 : G_1 \times G_2 \rightarrow \mathbb{C}^\times, \quad (g_1, g_2) \mapsto \chi_1(g_1)\chi_2(g_2).$$

It is easy to check that this map is a homomorphism, so $\chi_1 \times \chi_2 \in \widehat{G_1 \times G_2}$. Next, one checks easily that the map

$$(6.2) \quad \widehat{\widehat{G_1} \times \widehat{G_2}} \rightarrow \widehat{G_1 \times G_2}, \quad (\chi_1, \chi_2) \mapsto \chi_1 \times \chi_2$$

is a homomorphism. The kernel of (6.2) is trivial (for if $\chi_1 \times \chi_2(g_1, g_2) = \chi_1(g_1)\chi_2(g_2) = 1$ for all $(g_1, g_2) \in G_1 \times G_2$, restricting to $g_1 = 1$ or $g_2 = 1$ yields both $\chi_1 = 1$ and $\chi_2 = 1$, the trivial character on G_1 and on G_2 respectively). Finally, the map (6.2) is surjective. (For if $\chi \in \widehat{G_1 \times G_2}$, then restriction to the two factors gives homomorphisms $\chi_1(g_1) = \chi(g_1, 1)$ and $\chi_2(g_2) = \chi(1, g_2)$ and clearly $\chi_1 \times \chi_2 = \chi$.) So the map (6.2) is an isomorphism, and (a) follows.

For (b), we use the Fundamental Theorem of Finite Abelian Groups: Every finite abelian group is isomorphic to a direct product of finite cyclic groups. Thus it suffices to consider the case G is finite cyclic; and then (b) will follow in the general case using (a) for the inductive step.

Suppose thus that G is cyclic of order n , with generator x . Every homomorphism $\chi : G \rightarrow \mathbb{C}^\times$ is uniquely determined by its value $\chi(x)$ at the generator x , since $\chi(x^j) = \chi(x)^j$. One particular character is given by $\chi_1(x) = \zeta$ where $\zeta = \zeta_n = e^{2\pi i/n}$; here $\chi_1(x^j) = \zeta^j$. In this case we easily prove that $\langle \chi_1 \rangle = \widehat{G}$. For given any homomorphism $\chi : G \rightarrow \mathbb{C}^\times$, the value $\chi(x)$ is a complex root of unity, so $\chi(x) = \zeta^r = \chi_1(x)^r$ for some $r \in \{0, 1, 2, \dots, n-1\}$, whence $\chi = \chi_1^r$. Thus $\widehat{G} = \langle \chi_1 \rangle$ which is cyclic of order n . By induction (on the number of direct factors in G), (b) holds also in the general case. \square

The isomorphism $G \xrightarrow{\cong} \widehat{G}$ is *not canonical*. For example if $G = \langle x \rangle$ is cyclic of order 4, the dual group $\widehat{G} = \langle \chi_1 \rangle$ is also cyclic of order 4 where $\chi_1(x) = i = \sqrt{-1}$. However there is no algebraic property distinguishing i from $-i$ (the other principal fourth root of unity in \mathbb{C}). There are the two isomorphisms $G \rightarrow \widehat{G}$, one mapping $x \mapsto \chi_1$ and the other mapping $x \mapsto \overline{\chi_1}$; and there is no way to distinguish one of these as the ‘preferred’ isomorphism. The situation is quite like what we find in linear algebra: If V is a finite-dimensional vector space over a field F , then the dual space V^* is a vector space over F having the same dimension as V , so we must have $V^* \cong V$; however there is no canonical choice of vector space isomorphism $V \xrightarrow{\cong} V^*$. Any choice of isomorphism requires that we fix particular choices of ordered bases for V and for V^* .

Theorem 6.3. Given $\chi, \chi' \in \widehat{G}$ where $|G| = n$, we have

$$(a) \quad \sum_{g \in G} \chi'(g) \overline{\chi(g)} = \begin{cases} n, & \text{if } \chi = \chi'; \\ 0, & \text{otherwise.} \end{cases}$$

Dually, given $g, g' \in G$, we have

$$(b) \quad \sum_{\chi \in \widehat{G}} \chi(g') \overline{\chi(g)} = \begin{cases} n, & \text{if } g = g'; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Since $|\chi(g)| = 1$, it is clear that $\sum_{g \in G} |\chi(g)|^2 = n$ for $\chi \in \widehat{G}$. Now suppose that $\chi' \neq \chi$ in \widehat{G} , and let $S = \sum_{g \in G} \chi'(g) \overline{\chi(g)}$. Substituting $g = uh$ where $u \in G$ is fixed and h varies over G ,

$$S = \sum_{h \in G} \chi'(uh) \overline{\chi(uh)} = \chi'(u) \overline{\chi(u)} \sum_{h \in G} \chi'(h) \overline{\chi(h)} = \frac{\chi'(u)}{\chi(u)} S.$$

Since $\chi' \neq \chi$, there exists $u \in G$ such that $\chi'(u) \neq \chi(u)$, and this forces $S = 0$. This proves the orthogonality relations (a), which may be interpreted as saying that $AA^* = nI$ where A is the $n \times n$ matrix with rows and columns indexed by \widehat{G} and G respectively, having (χ, g) -entry equal to $\chi(g)$; and A^* is the conjugate transpose of A . Equivalently, the matrix $\frac{1}{\sqrt{n}}A$ is unitary, and so we also have $A^*A = nI$. This yields the second set of orthogonality relations (b). \square

The **group algebra** $\mathbb{C}[G]$ is the set of all formal linear combinations of elements of G with complex coefficients. This is a complex vector space of dimension $n = |G|$ having G as basis; but it is also a ring with multiplication defined as in G , as extended uniquely to $\mathbb{C}[G]$ by the distributive law. To be explicit, let $\alpha, \beta \in \mathbb{C}[G]$ be given by

$$\alpha = \sum_{g \in G} a_g g, \quad \beta = \sum_{g \in G} b_g g$$

where $a_g, b_g \in \mathbb{C}$ for all $g \in G$; then

$$\alpha\beta = \sum_{x, y \in G} a_x b_y xy = \sum_{g \in G} \left(\sum_{h \in G} a_{gh^{-1}} b_h \right) g \in \mathbb{C}[G]$$

after substituting $(x, y) = (gh^{-1}, h)$. Thus it is natural to consider the **convolution** of two functions $f_1, f_2 : G \rightarrow \mathbb{C}$; this is the function $f_1 * f_2 : G \rightarrow \mathbb{C}$ defined by

$$(f_1 * f_2)(g) = \sum_{h \in G} f_1(gh^{-1})f_2(h).$$

This works fine for a general finite group G , although here we only consider the case G is abelian. Now if we define

$$\widehat{f} = \sum_{g \in G} f(g)g \in \mathbb{C}[G]$$

for any function $f : G \rightarrow \mathbb{C}$, then the identity

$$\widehat{f_1 f_2} = \widehat{f_1 * f_2}$$

holds in $\mathbb{C}[G]$.

We now consider three complex inner product spaces of dimension $n = |G| = |\widehat{G}|$, as follows: The space $L^2(G)$ consists of all functions $G \rightarrow \mathbb{C}$ with inner product

$$[f_1, f_2] = \sum_{g \in G} f_1(g) \overline{f_2(g)}.$$

The space $L^2(\widehat{G})$ consists of all functions $\widehat{G} \rightarrow \mathbb{C}$ with inner product

$$[F_1, F_2] = \frac{1}{n} \sum_{\chi \in \widehat{G}} F_1(\chi) \overline{F_2(\chi)}.$$

The group algebra $\mathbb{C}[G]$ has inner product

$$[\alpha, \beta] = \sum_{g \in G} a_g \overline{b_g}$$

where $\alpha = \sum_{g \in G} a_g g$, $\beta = \sum_{g \in G} b_g g$. We have a commutative diagram of vector space isomorphisms

$$\begin{array}{ccc} L^2(G) & \xrightarrow{\mathcal{F}} & L^2(\widehat{G}) \\ & \searrow \iota & \nearrow \widehat{\iota} \\ & \mathbb{C}[G] & \end{array}$$

where $\iota(f) = \widehat{f}$ as defined above. Each $g \in G$ yields a natural function $g^* : \widehat{G} \rightarrow \mathbb{C}$, namely the evaluation $g^*(\chi) = \chi(g)$; and the map $\widehat{\iota} : G \rightarrow L^2(\widehat{G})$, $g \mapsto g^*$ has a unique linear extension to $\widehat{\iota} : \mathbb{C}[G] \rightarrow L^2(\widehat{G})$. The **Fourier transform** is the map $\mathcal{F} = \widehat{\iota} \circ \iota : L^2(G) \rightarrow L^2(\widehat{G})$ defined as follows: Given $f : G \rightarrow \mathbb{C}$, the map $\mathcal{F}f : \widehat{G} \rightarrow \mathbb{C}$ is given by

$$(\mathcal{F}f)(\chi) = \sum_{g \in G} f(g)\chi(g).$$

All three of these vector space isomorphisms are in fact isometries. To see for example that \mathcal{F} is an isometry, let $f_1, f_2 : G \rightarrow \mathbb{C}$, so that

$$\begin{aligned} [\mathcal{F}f_1, \mathcal{F}f_2] &= \frac{1}{n} \sum_{\chi \in \widehat{G}} (\mathcal{F}f_1)(\chi) \overline{(\mathcal{F}f_2)(\chi)} = \frac{1}{n} \sum_{\chi \in \widehat{G}} \sum_{g, h \in G} f_1(g)\chi(g) \overline{f_2(h)\chi(h)} \\ &= \frac{1}{n} \sum_{g, h \in G} f_1(g) \overline{f_2(h)} \delta_{g, h} n = \sum_{g \in G} f_1(g) \overline{f_2(g)} = [f_1, f_2] \end{aligned}$$

using Theorem 6.3(b). The identity $\widehat{f_1 f_2} = \widehat{f_1 * f_2}$ shows that ι is not only an isometry, but also an algebra isomorphism from $L^2(G)$ (under convolution) to $\mathbb{C}[G]$. All three edges of our commutative triangle are algebra isomorphisms if we endow $L^2(\widehat{G})$ with pointwise multiplication: for $F_1, F_2 : \widehat{G} \rightarrow \mathbb{C}$, $(F_1 F_2)(\chi) = F_1(\chi) F_2(\chi)$. Now given $f_1, f_2 : G \rightarrow \mathbb{C}$ and $\chi \in \widehat{G}$, we have

$$\begin{aligned} \mathcal{F}(f_1 * f_2)(\chi) &= \sum_{g \in G} \widehat{f_1 * f_2}(g) \chi(g) = \sum_{g, h \in G} f_1(gh^{-1}) f_2(h) \chi(g) = \sum_{x, y \in G} f_1(x) f_2(y) \chi(xy) \\ &= \sum_{x \in G} f_1(x) \chi(x) \sum_{y \in G} f_2(y) \chi(y) = (\mathcal{F}f_1)(\chi) (\mathcal{F}f_2)(\chi) \end{aligned}$$

so that $\mathcal{F}(f_1 * f_2) = (\mathcal{F}f_1)(\mathcal{F}f_2)$ as required. We have proved

Theorem 6.4. The three algebras $L^2(G)$ (with convolution), $L^2(\widehat{G})$ (with pointwise multiplication) and $\mathbb{C}[G]$ are isometrically isomorphic. In particular,

$$\mathbb{C}[G] \cong \mathbb{C}^n = \underbrace{\mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{n \text{ times}}$$

where \mathbb{C}^n has coordinatewise ring operations and the standard complex inner product. \square

Expositions of this topic vary widely between different sources, both in the extent of generality as well as in presentation style, depending on the author's tastes; and I have chosen the approach which best suits our particular theme and goals. Two directions in which the Fourier transform generalizes are to the case G is nonabelian, and the case G is infinite. When G is nonabelian, of course $\mathbb{C}[G] \not\cong \mathbb{C}^n$ since the group algebra $\mathbb{C}[G]$ is no longer commutative; and instead one finds that $\mathbb{C}[G]$ is isomorphic to a direct sum of full matrix algebras. This is the realm of **representation theory**; see e.g. [Is], [Se]. Much of this theory carries over in the infinite case, with more evident ease and success when G is a compact topological group, particularly a Lie group; or an algebraic group. See e.g. [BD]. The group algebra formulation $\mathbb{C}[G]$ is not really suitable in the infinite case, and so this member of the triangle is understandably absent, where one makes do with $L^2(G)$ (as an algebra under convolution) instead. See Exercise #5 for the standard example with $G = S^1$.

As an algebra, \mathbb{C}^n has 2^n **idempotent** elements (i.e. elements satisfying $\varepsilon^2 = \varepsilon$); these are the vectors having all components either 0 or 1. It also has exactly n primitive idempotents, these being the standard basis vectors of \mathbb{C}^n . (A **primitive idempotent** is a nonzero idempotent which is *not* expressible as $\varepsilon = \varepsilon_1 + \varepsilon_2$ where ε_1 and ε_2 are also nonzero idempotents.) Every idempotent is uniquely expressible as a sum of distinct primitive idempotents. In view of the isomorphisms above, $\mathbb{C}[G]$ must also have a basis consisting of n primitive idempotents.

Theorem 6.5. The primitive idempotents of $\mathbb{C}[G]$ are the elements $\frac{1}{n}\widehat{\chi} = \frac{1}{n}\sum_{g \in G} \chi(g)g$ for $\chi \in \widehat{G}$.

Proof. For $\chi, \psi \in \widehat{G}$ we have

$$\begin{aligned} \frac{1}{n}\widehat{\chi}\frac{1}{n}\widehat{\psi} &= \frac{1}{n^2}\sum_{x,y \in G} \chi(x)\psi(y)xy = \frac{1}{n^2}\sum_{g,h \in G} \chi(gh^{-1})\psi(h)g = \frac{1}{n^2}\sum_{g \in G} \chi(g)\left(\sum_{h \in G} \overline{\chi(h)}\psi(h)\right)g \\ &= \frac{1}{n^2}\sum_{g \in G} \chi(g)\delta_{\chi,\psi}ng = \delta_{\chi,\psi}\frac{1}{n}\widehat{\chi} \end{aligned}$$

using Theorem 6.3(a). These relations uniquely characterize the n primitive idempotents of $\mathbb{C}[G] \cong \mathbb{C}^n$. \square

Spectra of Cayley Graphs and Digraphs

As an application, we determine the spectra of Cayley graphs and digraphs over finite abelian groups. Although we do not consider loops or multiple edges, our presentation easily adapts to this more general setting. As above, G is a finite multiplicative abelian group. For an arbitrary subset $S \subseteq G$, consider the graph with vertex set G and edges (x, xs) whenever $x \in G$ and $s \in S$; thus (x, y) is an edge iff $x^{-1}y \in S$. This graph on $n = |G|$ vertices, with out-degree $|S|$ for every vertex, is the **Cayley digraph** $\Gamma = \Gamma(G, S)$.

We often require $1 \notin S$; otherwise Γ has a loop at every vertex. If we want Γ to be an ordinary graph, we would also require $s^{-1} \in S$ whenever $s \in S$. Note that Γ is connected (and in the directed case, strongly connected) iff $\langle S \rangle = G$. The **adjacency operator** $A : \mathbb{C}[G] \rightarrow \mathbb{C}[G]$ is the map $\alpha \mapsto \sigma\alpha$ where $\sigma = \sum_{s \in S} s \in \mathbb{C}[G]$. The **spectrum** (i.e. multiset of eigenvalues) of Γ is really the spectrum of the operator A . (Note that the matrix of A with respect to G , the standard basis of $\mathbb{C}[G]$, is the usual adjacency matrix of the graph Γ .)

Theorem 6.6. The n eigenvalues of Γ are the values $\chi(\sigma) = \sum_{s \in S} \chi(s)$ for $\chi \in \widehat{G}$.

We observe that these eigenvalues all lie in the ring $\mathbb{Z}[\zeta_m]$ where m is the exponent of G since, as we previously observed, all character values lie in this ring. Cayley graphs (and digraphs) of nonabelian finite groups also have eigenvalues consisting of cyclotomic integers since all character values lie in $\mathbb{Z}[\zeta_m]$ (although characters are defined somewhat differently, and the eigenvalues are computed by a rather more subtle process. In the case Γ is an ordinary graph (i.e. $s^{-1} \in S$ whenever $s \in S$), it is not hard to see that Theorem 6.6 gives real eigenvalues as expected: characters whose values extend outside $\{\pm 1\}$ occur in complex conjugate pairs, so their net contribution to the sum in Theorem 6.6 yields real values. So in the case of ordinary Cayley graphs, the eigenvalues of Γ lie in $\mathbb{Q}[\zeta_m] \cap \mathbb{R} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}]$.

Proof of Theorem 6.6. We show that the primitive idempotents of $\mathbb{C}[G]$ form a basis consisting of eigenvectors for A , with the indicated eigenvalues. In place of the primitive idempotents $\frac{1}{n}\widehat{\chi}$ we may of course use the scalar multiples $\widehat{\chi}$, $\chi \in \widehat{G}$. For each $\chi \in \widehat{G}$,

$$A\widehat{\chi} = \sum_{s \in S} s \sum_{g \in G} \chi(g)g = \sum_{s \in S} \sum_{x \in G} \chi(s^{-1}x)x = \overline{\chi(\sigma)} \sum_{x \in G} \chi(x)x = \overline{\chi(\sigma)}\widehat{\chi}.$$

So $\mathbb{C}[G]$ has a basis of eigenvectors for A , with corresponding eigenvalues $\overline{\chi(\sigma)}$, $\chi \in \widehat{G}$. Now complex conjugation permutes the characters of G ; so after reparameterizing, we obtain exactly the eigenvalues claimed. \square

Error-Correcting Codes

A second application of group characters is to the theory of error-correcting codes. Let $F = \mathbb{F}_q$, and fix $n \geq 1$. The **(Hamming) weight** of a vector $v = (v_1, v_2, \dots, v_n) \in F^n$, denoted by $\text{wt}(v)$, is the number of nonzero coordinates in v ; thus for example, the vector $(1, 0, 1, 1, 1, 0) \in F^6$ has $\text{wt}(v) = 4$. A **linear $[n, k]$ -code** is a k -dimensional subspace $\mathcal{C} \leq F^n$. Vectors in F^n are **words**; and vectors in \mathcal{C} are **codewords**. The **weight distribution** of the code \mathcal{C} is the sequence $A_0, A_1, A_2, \dots, A_n$ where $A_i = |\{v \in \mathcal{C} : \text{wt}(v) = i\}|$. The **minimum weight** of \mathcal{C} is the smallest $d \geq 1$ such that $A_d \neq 0$ (i.e. the smallest weight of any nonzero codeword). By linearity, the **minimum distance** of \mathcal{C} (the minimum

number of coordinates in which two distinct codewords differ) coincides with the minimum weight d .

Let us briefly summarize the key concepts of the theory of error-correcting codes (although this does injustice to such an extensive subject!) Words of length n are vectors $v \in F^n$ whose coordinates are regarded as sequences of n letter symbols from some finite **alphabet** (in this case F) used in information exchange. We may view \mathcal{C} as the row space of a $k \times n$ matrix B of full rank over F . The matrix B is the **generator matrix** of the code. (It is usually denoted G ; but we reserve ‘ G ’ for groups.) Now $\mathcal{C} = \{uB : u \in F^k\}$ where we regard each vector $u \in F^k$ as a plaintext message, and $uB \in \mathcal{C}$ as its corresponding codeword. The isomorphism $F^k \rightarrow \mathcal{C}$ is the **encoding** process. The purpose of such encoding is to protect against loss of information due to a limited number of errors during transmission between two parties (a ‘transmitter’ T and a ‘receiver’ R) in a noisy channel. Before transmitting the message $u \in F^k$, T first encodes it as $v = uB \in \mathcal{C}$ and sends this codeword. If R correctly receives v , all is well. If R instead receives $v' \in F^n$, a slightly corrupted version of v , then R can hope to correctly deduce the original transmitted word v (and thereby u) if $v \in \mathcal{C}$ is the unique codeword satisfying $\text{wt}(v - v') \leq e$ where e is sufficiently small. Indeed if $e = \lfloor \frac{d-1}{2} \rfloor$, then for every word $w \in \mathcal{C}$, there is at most one $v \in \mathcal{C}$ satisfying $\text{wt}(w-v) \leq e$. In this case, \mathcal{C} is an **e -error correcting code of length n** . The goal is to construct codes of a given length n over an alphabet of given size q , with the number of codewords q^k as large as possible (thereby ensuring a large **information rate**), yet with minimum distance d as large as possible (thereby maximizing the error-correcting capability e). These constraints, however, compete against each other; and a great deal of mathematics is used to look for the optimal code for a given set of parameters n, q , etc. There are other design considerations as well, which we have not mentioned. In particular, why must the alphabet be a finite field F , and the code a subspace of F^n ? For some parameter sets there are in fact nonlinear codes (non-subspaces) which perform slightly better than any linear code with the same parameters; but these are harder to design and to work with. Moreover any code, in order to be of practical value, must admit efficient algorithms for both encoding and decoding. Given these constraints, linear codes are generally the best bet for information exchange.

In addition to the generator matrix B introduced above, every $[n, k]$ -code over F can also be defined as the null space of an $(n - k) \times n$ matrix H over F :

$$\mathcal{C} = \{v \in F^n : Hv^T = 0\}.$$

Here H is the **parity check matrix** of \mathcal{C} ; it has full rank $n - k$. The parity check matrix H is useful for decoding: R uses it to check whether a word v is a valid codeword. The vector Hw^T is the **error syndrome** of the word $w \in F^n$. If $Hw^T = 0$, then w is a certified codeword; if $Hw^T \neq 0$, then the syndrome may yield useful information in locating the codeword closest to w .

Now the two matrices B and H play roles dual to each other: the row space of B is \mathcal{C} , while the row space of H is the **dual code**

$$\mathcal{C}^\perp = \{v \in F^n : wv^T = 0 \text{ for all } w \in \mathcal{C}\}.$$

Note that wv^T is the usual ‘dot product’ of two row vectors $v, w \in F^n$. While \mathcal{C} is an $[n, k]$ -code with generator matrix B and parity check matrix H , the dual code \mathcal{C}^\perp is an $[n, n-k]$ -code with generator matrix H and parity check matrix B . There is also a relationship between the weight distributions of these two codes (and in particular between their minimum weights). Please note however that while \mathcal{C} and \mathcal{C}^\perp must have complementary dimensions, they are not in general complementary subspaces; see Example 6.7 below.

The relationship between the weight distribution of a code and its dual (Theorem 6.8) is expressed most naturally in terms of their weight enumerators. For a code \mathcal{C} as above, the **weight enumerator** of \mathcal{C} is the polynomial

$$A_{\mathcal{C}}(x, y) = \sum_{v \in \mathcal{C}} x^{n-\text{wt}(v)} y^{\text{wt}(v)} = \sum_{d=0}^n A_d x^{n-d} y^d \in \mathbb{Z}[x, y].$$

Example 6.7: A Code and its Dual. Let $q = 2$, $F = \mathbb{F}_2$, and let $\mathcal{C} < F^5$ be the $[5, 2]$ -code spanned by 10111 and 01110. The dual code \mathcal{C}^\perp is the $[5, 3]$ -code spanned by 10001, 01011 and 00110. Since

$$\mathcal{C} = \{00000, 10111, 01110, 11001\}, \quad \mathcal{C}^\perp = \{00000, 10001, 01011, 00110, 11010, 10111, 01101, 11100\}$$

we obtain $A_{\mathcal{C}}(x, y) = x^5 + 2x^2y^3 + xy^4$, $A_{\mathcal{C}^\perp}(x, y) = x^5 + 2x^3y^2 + 4x^2y^3 + xy^4$. Following Theorem 6.8, we obtain either weight enumerator from the other via

$$\frac{1}{4}A_{\mathcal{C}}(x+y, x-y) = A_{\mathcal{C}^\perp}(x, y); \quad \frac{1}{8}A_{\mathcal{C}^\perp}(x+y, x-y) = A_{\mathcal{C}}(x, y)$$

which can be verified by direct computation. The code \mathcal{C} has minimum distance 3, the best (largest) possible for a $[5, 2]$ -code over \mathbb{F}_2 . It is 1-error correcting. Note that the word 10111 lies in $\mathcal{C} \cap \mathcal{C}^\perp$; so although \mathcal{C} and \mathcal{C}^\perp have complementary dimensions, they are not complementary subspaces.

Theorem 6.8 (MacWilliams). Let \mathcal{C} be a linear $[n, k]$ -code over $F = \mathbb{F}_q$. Then the weight enumerators of \mathcal{C} and its dual are related by

$$A_{\mathcal{C}^\perp}(x, y) = \frac{1}{q^k} A_{\mathcal{C}}(x + (q-1)y, x - y).$$

Proof. Fix a nontrivial character χ of the additive group of F . Thus $\chi : F \rightarrow \langle \zeta_p \rangle$ satisfies $\chi(a + b) = \chi(a)\chi(b)$. (Although we use an additive group F here rather than multiplicative, this presents none of the notational difficulties alluded to earlier, since the group algebra does not appear directly in this argument.) For all $u \in F^n$, define $g(u) = \sum_{v \in F^n} \chi(uv^T) x^{n-\text{wt}(v)} y^{\text{wt}(v)}$. Then

$$\begin{aligned} \sum_{u \in \mathcal{C}} g(u) &= \sum_{u \in \mathcal{C}} \sum_{v \in F^n} \chi(uv^T) x^{n-\text{wt}(v)} y^{\text{wt}(v)} \\ &= \sum_{v \in F^n} \left[\sum_{u \in \mathcal{C}} \chi(uv^T) \right] x^{n-\text{wt}(v)} y^{\text{wt}(v)} = q^k A_{\mathcal{C}^\perp}(x, y) \end{aligned}$$

since the inner sum $\sum_{u \in \mathcal{C}} \chi(uv^T) = 0$ whenever $v \notin \mathcal{C}^\perp$ (for such vectors v , the dot product uv^T yields each value of F the same number of times); whereas for $v \in \mathcal{C}^\perp$, we get a constant value $\chi(uv^T) = 1$ for all q^k choices of $u \in \mathcal{C}$. Now for $v = (v_1, v_2, \dots, v_n) \in F^n$, we have

$$\text{wt}(v) = \text{wt}(v_1) + \text{wt}(v_2) + \dots + \text{wt}(v_n) \quad \text{where } \text{wt}(v_i) = \begin{cases} 1, & \text{if } v_i \neq 0; \\ 0, & \text{if } v_i = 0 \end{cases}$$

and so

$$\begin{aligned} g(u) &= \sum_{v_1, v_2, \dots, v_n \in F} \chi(u_1 v_1 + u_2 v_2 + \dots + u_n v_n) x^{n-\text{wt}(u_1)-\text{wt}(u_2)-\dots-\text{wt}(u_n)} y^{\text{wt}(u_1)+\text{wt}(u_2)+\dots+\text{wt}(u_n)} \\ &= \sum_{v_1, v_2, \dots, v_n \in F} \chi(u_1 v_1) x^{1-\text{wt}(v_1)} y^{\text{wt}(v_1)} \chi(u_2 v_2) x^{1-\text{wt}(v_2)} y^{\text{wt}(v_2)} \dots \chi(u_n v_n) x^{1-\text{wt}(v_n)} y^{\text{wt}(v_n)} \\ &= \prod_{i=1}^n \sum_{v_i \in F} \chi(u_i v_i) x^{1-\text{wt}(v_i)} y^{\text{wt}(v_i)}. \end{aligned}$$

The innermost sum equals $x + (q-1)y$ if $u_i = 0$, or $x - y$ if $u_i \neq 0$. Thus

$$g(u) = (x + (q-1)y)^{n-\text{wt}(u)} (x - y)^{\text{wt}(u)}.$$

Summing over $u \in \mathcal{C}$ gives $\mathcal{A}_{\mathcal{C}}(x + (q-1)y, x - y)$. □

The Fast Fourier Transform

The Fast Fourier Transform (FFT) was known to Gauss at least as early as 1805 (predating Fourier, after whom the transform has been named). More recently, it was rediscovered by many others, notably Cooley and Tukey (1965). The point is that the Discrete Fourier Transform (DFT) over a large finite group, viewed as a square matrix, may appear quite large, requiring extensive time (presumably by a computer) in its computation. However due to the highly structured nature of this matrix, this computation can be performed in fewer steps than one might at first suppose. It is this faster approach to computing the DFT that accounts for the name FFT. The importance of this speedup is due to the vast number of problems requiring DFT for their solution, and where computational time required would otherwise be expensive or prohibitive. We begin by describing how the FFT works. We then give an application to fast multiplication for polynomials and for integers.

Let $G = \mathbb{Z}/n\mathbb{Z}$ (note: additive notation here). The dual group is $\widehat{G} = \{\chi_j : j \in G\}$ where $\chi_j(k) = \zeta^{jk}$. The Fourier transform of an arbitrary function $f : G \rightarrow \mathbb{C}$ is $F = \mathcal{F}f$ where we abbreviate $F(\chi_j)$ by $F(j)$ to get

$$F(j) = \sum_{k \in G} f(k)\chi_j(k) = \sum_{k=0}^{n-1} \zeta_n^{jk} f(k).$$

The matrix of the Fourier transform is the matrix

$$H_n := (\zeta_n^{jk} : 0 \leq j, k < n)$$

which goes by many names: Fourier matrix, character table of the cyclic group of order n , generalized Sylvester matrix, etc. Of course it is also a particular Vandermonde matrix. And we will meet this matrix in Section 16 as the most classical construction of complex Hadamard matrix; hence our notation H_n for this matrix. A naive computer implementation of the Fourier transform entails multiplying H_n by a column vector in \mathbb{C}^n . This requires n^2 product operations in \mathbb{C} , plus several addition operations in \mathbb{C} . Scalar addition is much faster than scalar multiplication, so for simplicity we neglect them in saying

$$(6.9) \quad \text{the naive implementation of the Fourier transform } \mathcal{F} : L^2(G) \rightarrow L^2(\widehat{G}) \text{ requires } n^2 = 4m^2 \text{ scalar multiplications.}$$

Assume for the moment that G has even order, say $n = 2m$. To improve upon (6.9), represent f and $F = \mathcal{F}f$ by column vectors as

$$f \leftrightarrow \begin{bmatrix} f_{\text{even}} \\ f_{\text{odd}} \end{bmatrix} \quad \text{where } f_{\text{even}} = \begin{bmatrix} f(0) \\ f(2) \\ f(4) \\ \vdots \\ f(n-2) \end{bmatrix}, \quad f_{\text{odd}} = \begin{bmatrix} f(1) \\ f(3) \\ f(5) \\ \vdots \\ f(n-1) \end{bmatrix};$$

and dually,

$$F \leftrightarrow \begin{bmatrix} F_{\text{top}} \\ F_{\text{bottom}} \end{bmatrix} \quad \text{where } F_{\text{top}} = \begin{bmatrix} F(0) \\ F(1) \\ F(2) \\ \vdots \\ F(m-1) \end{bmatrix}, \quad F_{\text{bottom}} = \begin{bmatrix} F(m) \\ F(m+1) \\ F(m+2) \\ \vdots \\ F(2m-1) \end{bmatrix}.$$

Note that we have indexed entries of F in the usual way; but the coordinates of f have been indexed differently, starting with the even coordinates (expressing the restriction of f to the subgroup of G of index 2), followed by the odd coordinates (where f is restricted to the other coset of that subgroup). The reason we say ‘dually’, and why this is the *right* thing to do, is that the vectors F_{top} and F_{bottom} list the values of F on cosets of the subgroup $\langle \chi_m \rangle$ of order 2 in \widehat{G} . With respect to this indexing of the rows and columns, the Fourier transform is takes the form

$$(6.10) \quad \begin{bmatrix} F_{\text{top}} \\ F_{\text{bottom}} \end{bmatrix} = \begin{bmatrix} H_m & D_m H_m \\ H_m & -D_m H_m \end{bmatrix} \begin{bmatrix} f_{\text{even}} \\ f_{\text{odd}} \end{bmatrix}, \quad \text{i.e.} \quad \begin{cases} F_{\text{top}} = H_m f_{\text{even}} + D_m H_m f_{\text{odd}}; \\ F_{\text{bottom}} = H_m f_{\text{even}} - D_m H_m f_{\text{odd}} \end{cases}$$

where $H_m = (\zeta_m^{jk} : j, k \in \mathbb{Z}/m\mathbb{Z})$ and $D_m = \text{diag}(1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1})$. Computing $H_m f_{\text{even}}$ requires only m^2 scalar multiplications, as does $H_m f_{\text{odd}}$; and then left-multiplication by D_m requires an additional scalar multiplications. Once again, the faster operations of scalar addition have been neglected here. Thus

$$(6.11) \quad \text{implementation of the Fourier transform } \mathcal{F} : L^2(G) \rightarrow L^2(\widehat{G}) \text{ using (6.10) requires only } 2m^2 + m \text{ scalar multiplications.}$$

Note that the improvement from (6.9) to (6.11) is a reduction in execution time, almost by a factor of two. Similar gains are found using an arbitrary small prime divisor $p \mid n$ in place of the prime 2. Now note that the main step in implementing (6.10) is the application of H_m , which can be similarly reduced to $H_{m'}$ where $m = 2m'$, or $m = pm'$ using another small prime p dividing m , to obtain further speedup. Assuming the original n is a product of small primes, iterating this reduction significantly improves execution time. Notably,

$$(6.12) \quad \text{when } n = 2^k, \text{ using } k \text{ iterations of the reduction described above, the Fourier transform over } G = \mathbb{Z}/n\mathbb{Z} \text{ requires only } O(n \log n) \text{ scalar multiplications as compared with } O(n^2) \text{ scalar multiplications using the direct approach (6.9).}$$

This is the idea of the FFT. Its applications are far too ubiquitous to be summarized here. We content ourselves with describing two of the many applications of FFT.

Fast Polynomial Multiplication

Consider now the problem of multiplying two polynomials $f(x), g(x) \in \mathbb{C}[x]$. Choose $n > 2 \max\{\deg f(x), \deg g(x)\}$, so that $f(x)g(x) \in \mathbb{C}[x]$ has degree less than n . For simplicity we will take n to be the smallest power of 2 exceeding $\max\{\deg f(x), \deg g(x)\}$. (We could do better by finding another round number $n > \max\{\deg f(x), \deg g(x)\}$ divisible mostly by small primes, but $n = 2^k$ is almost optimal; and to do better could never improve our execution time by a factor > 2 . Such an improvement would be small compared to the improvement available using FFT with $n = 2^k$.)

The naive implementation of polynomial multiplication of polynomial multiplication $f(x)g(x)$ requires $O(n^2)$ operations of scalar multiplication in \mathbb{C} —we multiply each coefficient in $f(x)$ by each coefficient in $g(x)$. Again, we don't worry about scalar additions.

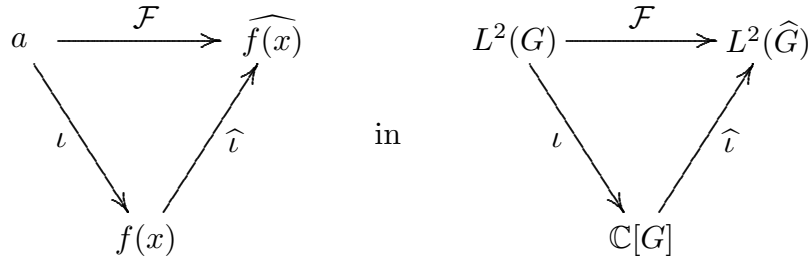
To do better, we work with a multiplicative cyclic group $G = \{1, x, x^2, \dots, x^{n-1}\}$ of order n . Noting that $\mathbb{C}[G] \cong \mathbb{C}[x]/(x^n - 1)$, we work with the images of $f(x)$ and $g(x)$ in this quotient ring. Because n was chosen large enough, the product $f(x)g(x)$ as computed

in $\mathbb{C}[G]$ (reduced mod $(x^n - 1)$) is the same as the answer in $\mathbb{C}[x]$. The algorithm to compute this product, improving upon the naive approach, is as follows.

- (I) First compute $\widehat{f(x)} \in L^2(\widehat{G})$. This is the Fourier transform of the sequence of coefficients in $f(x)$, requiring $O(n \log n)$ operations using FFT. Similarly compute $\widehat{g(x)} \in L^2(\widehat{G})$, which also requires $O(n \log n)$ operations.
- (II) Multiply to obtain $\widehat{f(x)g(x)}$ in $L^2(\widehat{G}) \cong \mathbb{C}^n$. This requires $O(n)$ scalar multiplications in \mathbb{C} . Note that $\widehat{f(x)g(x)} = \widehat{f(x)}\widehat{g(x)}$.
- (III) Compute $f(x)g(x) \in \mathbb{C}[G]$ by applying $\widehat{\iota}$ to $\widehat{f(x)g(x)}$. This takes another $O(n \log n)$ steps using FFT.

The total execution time to compute $f(x)g(x) \in \mathbb{C}[x]$ this way is $O(3n \log n + n) = O(n \log n)$ operations, as compared with $O(n^2)$ operations by the naive approach.

Some clarification: If $f(x) = \sum_{k=0}^{n-1} a_k x^k \in \mathbb{C}[x]$ then the sequence of coefficients is viewed as a function $a : G \rightarrow \mathbb{C}$, $x^k \rightarrow a_k$. Now $a \in L^2(G)$ and $f(x) = \iota(a) \in \mathbb{C}[G]$. Our careful use of notation may appear overly pedantic to the casual observer; but it serves to distinguish the function a (whose values are the coefficients in the polynomial $f(x)$) from the polynomial function f itself. The Fourier transform gives $\mathcal{F}a = \widehat{\iota}(f(x)) = \widehat{f(x)} \in L^2(\widehat{G})$. This completes the triangle



We have described the final step (III) above as a Fourier transform. It is actually the inverse of the Fourier transform $\mathcal{F} : L^2(G) \rightarrow L^2(\widehat{G})$, given by $\mathcal{F}^{-1} : L^2(\widehat{G}) \rightarrow L^2(G)$; but since $\widehat{\widehat{G}} \cong G$ (canonically), this is just the usual Fourier transform for the dual group \widehat{G} . The matrix expressing \mathcal{F}^{-1} as a linear transformation is $H_n^{-1} = H_n^* = \overline{H_n}$ since H_n is symmetric and unitary. Of course this is also a DFT; so it is efficiently computed using FFT (but for the dual group, so its coefficients are the complex conjugates of those in the FFT of step (I)).

Fast Integer Multiplication

We consider the computational complexity of multiplying two large integers exactly. For sufficiently small integers, most programming languages handle this perfectly well using the standard integer class of variables; for example $0, 1, 2, \dots, 4294967295$ can be handled quite well using 4-byte unsigned integers, for which multiplication is implemented directly by processor hardware. Larger integers requiring exact multiplication (e.g. in cryptographic applications) must be stored as arrays, and algorithms for fast multiplication are required.

Let M and N be two integers expressed in base b as $M = a_0 + a_1b + a_2b^2 + \cdots + a_{n-1}b^{n-1} = f(b)$ where $f(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}[x]$ and $a_i \in \{0, 1, 2, \dots, b-1\}$; and similarly $N = g(b)$. We take n sufficiently large that each of the numbers M , N and MN is expressible using at most n digits in base b notation. One first thinks $b = 2$ for binary or $b = 10$ for decimal; but it is better to use $b = 2^{16}$ or some such value in order to make best use of the hardware capabilities of the processor (see the comments below). Naive implementation requires $O(n^2)$ basic operations (not counting additions) to evaluate MN , since we multiply each digit in M by each digit in N .

In order to do better, we first evaluate the product of the two polynomials $f(x)g(x)$ in $O(n \log n)$ steps using Fast Polynomial Multiplication as described above. After obtaining $f(x)g(x) \in \mathbb{Z}[x]$, evaluate at $x = b$ and perform the necessary ‘carries’ (required whenever coefficients exceed the base b). The execution time required for this reduction is small compared to the Fast Polynomial Multiplication. Overall, we are able to perform Fast Integer Multiplication of n -digit integers in $O(n \log n)$ time steps.

Of course we have overlooked many details of the implementation. In particular one notes that the base b should actually be chosen somewhat smaller than the size of the native integer type of the processor, since coefficients of $f(x)g(x) \in \mathbb{Z}[x]$ will require slightly more than twice as many digits as coefficients in the original polynomials.

Exercises 6.

1. (a) Prove that for any finite group G , convolution of functions $G \rightarrow \mathbb{C}$ is associative; that is, $(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$ for all functions $f_1, f_2, f_3 \in G$. Can you obtain this result using known properties of the group algebra $\mathbb{C}[G]$? Explain.
 (b) Is the set of functions $G \rightarrow \mathbb{C}$ under convolution a group? Explain.
2. (a) Give an example of two finite abelian groups G_1 and G_2 of the same order, yet with $G_1 \not\cong G_2$.
 (b) If G_1 and G_2 are as in (a), are the corresponding group algebras $\mathbb{C}[G_1]$ and $\mathbb{C}[G_2]$ isomorphic? Explain.
3. Let $F = \mathbb{F}_3$, and consider the linear $[5, 2]$ -code \mathcal{C} spanned by the vectors 10012 and 01211.
 (a) Find a basis for the dual code \mathcal{C}^\perp .
 (b) Explicitly list all vectors in \mathcal{C} and in \mathcal{C}^\perp .
 (c) From (b), write down the explicit weight enumerators for \mathcal{C} and for \mathcal{C}^\perp .
 (d) By direct computation, verify that this example satisfies the MacWilliams relation (Theorem 6.8).
4. Find an ordinary graph Γ (undirected, with no loops or multiple edges), as small as possible, whose eigenvalues are not cyclotomic integers. Justify your answer.

Much of Section 6 generalizes to infinite groups; but this works best when G is a compact topological group. For a group G to be a topological group, one requires that G also have a topology compatible with the algebraic structure in the sense that the group multiplication $(g, h) \mapsto gh$ and the inverse map $g \mapsto g^{-1}$ are continuous. Compactness and commutativity together mean that we have a translation-invariant measure on G (Haar measure) with respect to which we can integrate. Here we give only the group $G = S^1$ as an example; and we stop short of providing a full account of the appropriate generalization of Theorem 6.4 to this situation.

5. Let G be the multiplicative group consisting of all $z \in \mathbb{C}$ such that $|z| = 1$. This is not a finite group, but it is abelian. As a topological space, G is homeomorphic to a circle (and in particular, G is compact). For $f_1, f_2 : G \rightarrow \mathbb{C}$, define $[f_1, f_2] = \int_G f_1(z) \overline{f_2(z)} \frac{dz}{iz} = \frac{1}{2\pi} \int_0^{2\pi} f_1(e^{ti}) \overline{f_2(e^{ti})} dt$.

The complex vector space $L^2(G)$ consists of all integrable functions $G \rightarrow \mathbb{C}$ having finite norm $\|f\| = \sqrt{[f, f]}$, but with two functions identified whenever they disagree on a set of measure zero. The **convolution** of two such functions is defined by

$$(f_1 * f_2)(w) = \int_{z \in G} f_1(wz^{-1}) \overline{f_2(z)} \frac{dz}{iz} = \frac{1}{2\pi} \int_0^{2\pi} f_1(we^{-ti}) \overline{f_2(e^{ti})} dt.$$

We have $\|f_1 * f_2\| < \infty$ whenever $\|f_i\| < \infty$; so the space $L^2(G)$ is closed under convolution (you may assume this).

- (a) Show that convolution is associative, i.e. $(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3)$ for all $f_1, f_2, f_3 \in L^2(G)$.
 (b) Find an infinite cyclic group $\{\chi_n : n \in \mathbb{Z}\}$ of homomorphisms $\chi_n : G \rightarrow \mathbb{C}^\times$. (As homomorphisms of topological groups, the maps $\chi_n : G \rightarrow \mathbb{C}^\times$ are required to be continuous as well as multiplicative.)

7. Group Rings $R[G]$

Section 6 includes a description of the group algebra $\mathbb{C}[G]$ of a finite abelian group G over the complex numbers. Replacing the coefficient ring \mathbb{C} by another choice of commutative ring R with identity, one similarly obtains the **group ring** $R[G]$ of G over R (or in the case R is actually a field, the **group algebra** over R). As before, the group G is assumed to be multiplicative. Despite conceptual convenience of complex number coefficients, \mathbb{C} suffers from some difficulties not evident with other rings. In particular, computer implementation of arithmetic in $\mathbb{C}[G]$ is fraught with difficulty due to numerical errors inherent in floating point approximation; whereas arithmetic in $\mathbb{Z}[G]$, or even in $\mathbb{Q}[G]$, can be implemented exactly if arbitrary precision arithmetic with coefficients is available—a realistic expectation in many programming languages. For many applications, this is a serious consideration. Another advantage of varying the coefficient ring R will appear below (see the comments following Corollary 7.3). For our purposes, taking R to be an **integral domain** (i.e. a commutative ring with identity having no zero divisors) is a quite adequate level of generality.

Every character $\chi \in \widehat{G}$ naturally extends to a homomorphism of algebras over \mathbb{Q} given by

$$\chi : \mathbb{Q}[G] \rightarrow \mathbb{Q}[\zeta_m], \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g \chi(g)$$

where m is the exponent of G (the least common multiple of the orders of the elements of G). It is easy to verify the required properties

$$\chi(a\alpha + b\beta) = a\chi(\alpha) + b\chi(\beta), \quad \chi(\alpha\beta) = \chi(\alpha)\chi(\beta) \quad \text{for all } \alpha, \beta \in \mathbb{Q}[G]$$

from the definitions. Now we must be wary when using the same letter χ to denote both a group homomorphism $G \rightarrow \mathbb{C}^\times$ and an algebra homomorphism $\mathbb{Q}[G] \rightarrow \mathbb{C}$; in particular these two maps have rather different kernels as given by

$$\ker(\chi : G \rightarrow \mathbb{C}^\times) = \{g \in G : \chi(g) = 1\}, \quad \ker(\chi : \mathbb{Q}[G] \rightarrow \mathbb{C}) = \{\alpha \in \mathbb{Q}[G] : \chi(\alpha) = 0\}.$$

But these two kernels are related; in particular for $g \in G$, we have $g \in \ker(\chi : G \rightarrow \mathbb{C}^\times)$ iff $g - 1 \in \ker(\chi : \mathbb{Q}[G] \rightarrow \mathbb{C})$. Rather than introduce a new letter for the algebra homomorphism, we shall try to clarify using context whenever the algebra homomorphism is intended; and *whenever we write simply $\ker \chi$, we mean the kernel of $\chi : G \rightarrow \mathbb{C}^\times$.*

The Rational Group Algebra of a Finite Cyclic Group

Suppose now that G is cyclic of order n . As indicated above, each $\chi \in \widehat{G}$ extends to an algebra homomorphism $\chi : \mathbb{Q}[G] \rightarrow \mathbb{Q}[\zeta_n]$; and in view of the isomorphism

$$(7.1) \quad \mathbb{Q}[G] \cong \mathbb{Q}[x]/(x^n - 1) \cong \bigoplus_{d|n} \mathbb{Q}[x]/(\Phi_d(x)) \cong \bigoplus_{d|n} \mathbb{Q}[\zeta_d],$$

χ then lifts to an algebra homomorphism $\mathbb{Q}[x] \rightarrow \mathbb{Q}[\zeta_n]$ whose kernel contains the ideal $(x^n - 1)$. Since the image of this map is evidently a subfield of $\mathbb{Q}[\zeta_n]$, this image is $\mathbb{Q}[\zeta_d]$ for some $d \mid n$. Now the kernel of the homomorphism $\mathbb{Q}[x] \rightarrow \mathbb{Q}[\zeta_d]$ induced by χ is the principal ideal $(\Phi_d(x)) \subset \mathbb{Q}[x]$. This means that the values of χ generate the cyclotomic extension $\mathbb{Q}[\zeta_d]$. Under the isomorphism $\mathbb{Q}[G] \cong \mathbb{Q}[x]/(x^n - 1)$ above, the monomial x corresponds to a generator g of G ; and then an arbitrary element $g^k \in G$ lies in $\ker \chi = \ker(\chi : G \rightarrow \mathbb{C}^\times)$, iff $g^k - 1$ lies in the kernel of $\chi : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\zeta_n]$, iff $x^k - 1$ is divisible by $\Phi_d(x)$, iff $d \mid k$. This shows that $[G : \ker \chi] = d$. We obtain

Theorem 7.2. Suppose G is cyclic of order n , and let $\chi \in \widehat{G}$ be a character of order d , so that $[G : \ker \chi] = d$. Then χ extends to an algebra homomorphism $\mathbb{Q}[G] \rightarrow \mathbb{Q}[\zeta_n]$ having image $\mathbb{Q}[\zeta_d]$ and kernel given by the principal ideal

$$\ker(\chi : \mathbb{Q}[G] \rightarrow \mathbb{Q}[\zeta_n]) = (\Phi_d(g)) \subseteq \mathbb{Q}[G]$$

where $\Phi_d(g) \in \mathbb{Q}[G]$ is the evaluation of the cyclotomic polynomial $\Phi_d(x)$ at a generator g of G . \square

Note that the parameter $d \mid n$ uniquely characterizes the kernel of the algebra homomorphism $\chi : \mathbb{Q}[G] \rightarrow \mathbb{C}$, as well as the kernel (and the order) of $\chi : G \rightarrow \mathbb{C}^\times$; however it does not uniquely characterize the image $\mathbb{Q}[\zeta_d]$ since for d odd, $\mathbb{Q}[\zeta_d] = \mathbb{Q}[\zeta_{2d}]$.

Corollary 7.3. Let G be a finite abelian group, and let $\alpha, \beta \in \mathbb{Q}[G]$. Then

- (a) $\alpha = \beta$ iff $\chi(\alpha) = \chi(\beta)$ for all $\chi \in \widehat{G}$.
- (b) Suppose G is cyclic of order n ; and for each $k \mid n$, consider the character $\chi_k \in \widehat{G}$ of order $d = \frac{n}{k}$. Then $\alpha = \beta$ iff $\chi_k(\alpha) = \chi_k(\beta)$ for all $k \mid n$.

The set $\mathcal{X} = \{\chi_k : k \mid n\}$ has cardinality $|\mathcal{X}| = \sigma(n)$, where $\sigma(n)$ is the number of positive integer divisors of n ; see Exercise #1.5. Note that $\sigma(n)$ is generally quite small compared with n . By comparison, given two elements $\alpha, \beta \in \mathbb{C}[G]$ where G is cyclic of order n , we have $\alpha = \beta$ iff $\chi(\alpha) = \chi(\beta)$ for all n characters $\chi \in \widehat{G}$. No fewer than all n characters will suffice for this purpose. Recall the algebra homomorphism $\mathbb{C}[G] \cong \mathbb{C}^n$; and note that each algebra homomorphism $\chi : \mathbb{C}[G] \rightarrow \mathbb{C}$, being \mathbb{C} -linear, has an $(n-1)$ -dimensional subspace as its kernel. The intersection of all these kernels is $\{0\}$; but for any proper subset $\mathcal{X} \subset \widehat{G}$ of size $|\mathcal{X}| = k < n$, the subspace $\bigcap_{\chi \in \mathcal{X}} \ker(\chi : \mathbb{C}[G] \rightarrow \mathbb{C}) \subseteq \mathbb{C}[G]$ has dimension $\geq n - k \geq 1$; it therefore contains $\alpha \neq 0$ satisfying $\chi(\alpha) = \chi(0) = 0$ for all $\chi \in \mathcal{X}$. Another way to say this is that over \mathbb{C} , the analogue of (7.1) is the algebra isomorphism $\mathbb{C}[G] \xrightarrow{\cong} \mathbb{C}^n$, $\alpha \mapsto (\chi(\alpha) : \chi \in \widehat{G})$. Each equation $\chi(\alpha) = \chi(\beta)$ says that two vectors in \mathbb{C}^n (corresponding to $\alpha, \beta \in \mathbb{C}[G]$) have two coordinates the same; but to guarantee equality of the two vectors, one must compare *all* n coordinates.

In practical implementations of Corollary 7.3 for the purpose of checking for equality of two elements of $\mathbb{Q}[G]$, it should be remembered (as previously observed) that each of the equalities $\chi_k(\alpha) = \chi_k(\beta)$ can be checked *exactly* using arbitrary precision arithmetic, in the ring $\mathbb{Q}[G] \cong \mathbb{Q}[x]/(x^n - 1)$. Nevertheless, since floating precision is typically much easier to implement and requires less execution time, it may be that when testing a large number of pairs (α, β) in $\mathbb{Q}[G]$ as candidates for equality, most of the cases can be ruled out quickly using floating point arithmetic; and only in those cases where numerical values agree to within a well-chosen tolerance, then closer inspection using exact arithmetic be used for a final check for equality.

Proof of Corollary 7.3. By Theorem 7.2, the isomorphism $\mathbb{Q}[G] \xrightarrow{\cong} \bigoplus_{d \mid n} \mathbb{Q}[\zeta_d]$ of (7.1) is explicitly given by $\alpha \mapsto (\chi_d(\alpha) : d \mid n)$. The fact that this map is injective is the desired conclusion. \square

Notational Accommodations for Additive Groups

We have described the construction of the group ring $R[G]$ of multiplicative group G over a suitable ring R . A notational difficulty arises when this construction is applied directly to an additive group G , since addition becomes ambiguous: we have two different types of addition, ring addition in $R[G]$ (where coefficients of like terms are added in R) and addition in G . Fortunately this difficulty is easily resolved, as we now describe.

Let G be an *additive group*. (Presumably G is *abelian*, as by popular convention, we always assume addition to be commutative; however this assumption is not strictly necessary.) We assume G has order $|G| = v$ and identity element $0 \in G$. Introduce v new symbols x^g , one for each group element $g \in G$, which we multiply according to the rule

$$x^g x^h = x^{g+h} \quad \text{for } g, h \in G.$$

This makes $X := \{x^g : g \in G\}$ a multiplicative group, isomorphic to G via the obvious correspondence $g \leftrightarrow x^g$. We also abbreviate $1 := x^0$ for the multiplicative identity element

of X . Now the group algebra of X (or of G) over R has addition and multiplication defined by

$$\sum_{g \in G} a_g x^g + \sum_{g \in G} b_g x^g = \sum_{g \in G} (a_g + b_g) x^g; \quad \left(\sum_{g \in G} a_g x^g \right) \left(\sum_{g \in G} b_g x^g \right) = \sum_{g \in G} \left(\sum_{h \in G} a_{g-h} b_h \right) x^g.$$

The group ring $R[X]$ of X over R works just like before; and we will often refer to this group ring as simply $R[G]$, implicitly invoking the isomorphism $X \cong G$, as this is merely a notational device.

Example 7.4: The Group Algebra $\mathbb{R}[\mathbb{Z}]$. The infinite additive cyclic group $G = \mathbb{Z}$ is rewritten multiplicatively as $X = \{x^k : k \in \mathbb{Z}\}$. The group ring (with real coefficients) takes the form $\mathbb{R}[G] = \mathbb{R}[X] = \mathbb{R}[x, x^{-1}]$ which is the **ring of Laurent polynomials with real coefficients**. It consists of all polynomials in x and x^{-1} (note: only finitely many terms, but exponents may be positive, negative or zero). This ring is of course an algebra over \mathbb{R} of infinite dimension, with X as basis.

Example 7.5: The Group Algebra $\mathbb{Q}[\mathbb{Z}/n\mathbb{Z}]$. The finite additive cyclic group $G = \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$ of order n is isomorphic to the finite multiplicative cyclic group $X = \{1, x, x^2, \dots, x^{n-1}\}$ where the generator x has order n . The group ring (with rational coefficients) is $\mathbb{Q}[G] = \{a_0 + a_1 x + \dots + a_{n-1} x^{n-1} : a_i \in \mathbb{Q}\} \cong \mathbb{Q}[x]/(x^n - 1)$, an algebra of dimension n .

Direct Products

Let G_1 and G_2 be multiplicative groups of order n_1 and n_2 respectively. The direct product $G_1 \times G_2$ is the group of order $n_1 n_2$ whose elements are ordered pairs (g_1, g_2) , $g_i \in G_i$. Multiplication is componentwise, viz. $(g_1, g_2)(g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$. We will identify G_1 and G_2 with the corresponding subgroups $G_1 \times \{1\}$ and $\{1\} \times G_2$ of $G_1 \times G_2$ via the embeddings $g_1 \mapsto (g_1, 1)$ and $g_2 \mapsto (1, g_2)$. (There is no harm or ambiguity in these identifications unless G_1 and G_2 contain nonidentity elements sharing the same symbols; but then we simply replace G_1 or G_2 by an isomorphic copy on a new set of symbols to avoid the ambiguity.) Now the embeddings $G_1, G_2 \subseteq G_1 \times G_2$ give rise to subalgebras $R[G_1]$ and $R[G_2]$ embedded in the group algebra $R[G_1 \times G_2]$; and the set of products of the form $\alpha_1 \alpha_2$, $\alpha_i \in R[G_i]$, serve to generate the entire algebra $R[G_1 \times G_2]$ as an R -module. Readers comfortable with tensor products will already recognize that this observation is more fully expressed by the isomorphism $R[G_1 \times G_2] \cong R[G_1] \otimes_R R[G_2]$; and readers unfamiliar with this terminology can safely shelve it for future reference.

Recall from Theorem 6.1(a) that every character $\chi \in \widehat{G_1 \times G_2}$ has the form $\chi = \chi_1 \times \chi_2$ where $\chi_i \in \widehat{G_i}$, so that $\chi(g_1, g_2) = \chi_1(g_1) \chi_2(g_2)$ whenever $g_i \in G_i$. This extends by \mathbb{Q} -linearity to the rational group algebra of $G_1 \times G_2$, so that if

$$\alpha = \sum_{j=1}^k r_j \alpha_{1,j} \alpha_{2,j} \in \mathbb{Q}[G_1 \times G_2], \quad r_j \in \mathbb{Q}, \quad \alpha_{i,j} \in \mathbb{Q}[G_i],$$

then

$$\chi(\alpha) = \sum_{j=1}^k r_j \chi_1(\alpha_{1,j}) \chi_2(\alpha_{2,j}) \in \mathbb{C}.$$

Example 7.6: $\mathbb{Q}[G_1 \times G_2]$ where G_1 and G_2 are finite cyclic. Let $G_1 = \{1, x, x^2, \dots, x^{m-1}\}$ be cyclic of order m , and $G_2 = \{1, y, y^2, \dots, y^{n-1}\}$ be cyclic of order n . Then $\mathbb{Q}[G_1 \times G_2] \cong \mathbb{Q}[x, y]/(x^m-1, y^n-1)$, an algebra of dimension mn over \mathbb{Q} . Note that $\mathbb{Q}[G_1] \cong \mathbb{Q}[x]/(x^m-1)$ and $\mathbb{Q}[G_2] \cong \mathbb{Q}[y]/(y^n-1)$; and we have simply tensored these two algebras together over \mathbb{Q} using $\mathbb{Q}[x, y] \cong \mathbb{Q}[x] \otimes_{\mathbb{Q}} \mathbb{Q}[y]$ and the remarks above. Here $\{x^i y^j : 0 \leq i < m, 0 \leq j < n\}$ is a basis over \mathbb{Q} . Similarly if $G_1 = \mathbb{Z}/m\mathbb{Z}$ and $G_2 = \mathbb{Z}/n\mathbb{Z}$, then replacing these additive cyclic groups by their multiplicative proxies as in Example 7.5, we once again have $\mathbb{Q}[G_1 \times G_2] \cong \mathbb{Q}[x, y]/(x^m-1, y^n-1)$.

Having established the necessary notational preliminaries, we discuss the important case of the additive group G of a finite field \mathbb{F}_q . Here G is elementary abelian of order q , and we are interested in the group algebra $\mathbb{Q}[G]$; but to simplify statements, all reference to X , the multiplicative copy of G , will be suppressed.

Theorem 7.7. Let G be the additive group of a finite field $F = \mathbb{F}_q$ of odd order. Let $S, N \subset G$ be the subsets of size $\frac{q-1}{2}$ corresponding to the nonzero squares and the nonsquares in F . Let $\alpha, \beta, \kappa \in \mathbb{Q}[G]$ denote the sums of S , N and G respectively, in the group algebra. Then α generates a 3-dimensional ideal in $\mathbb{Q}[G]$ with basis $\{1, \alpha, \beta\}$, or $\{1, \alpha, \kappa\}$. We have $\kappa = 1 + \alpha + \beta$; $\alpha\kappa = \beta\kappa = \frac{q-1}{2}\kappa$; $\kappa^2 = q\kappa$ and the following relations are satisfied.

- (a) If $q \equiv 1 \pmod{4}$: $\alpha^2 = \frac{q-1}{2} + \frac{q-5}{4}\alpha + \frac{q-1}{4}\beta = \frac{q-1}{4}(1 + \kappa) - \alpha$; $\alpha^* = \alpha$; $\beta^* = \beta$; every nontrivial $\chi \in \widehat{G}$ satisfies $\chi(\alpha) = \frac{1}{2}(-1 \pm \sqrt{q})$ and $\chi(\beta) = \frac{1}{2}(-1 \mp \sqrt{q})$.
- (b) If $q \equiv 3 \pmod{4}$: $\alpha^* = \beta$; $\alpha\alpha^* = \frac{q+1}{4} + \frac{q-3}{4}\kappa$; every nontrivial character $\chi \in \widehat{G}$ satisfies $\chi(\alpha) = \frac{1}{2}(-1 \pm i\sqrt{q})$ and $\chi(\beta) = \frac{1}{2}(-1 \mp i\sqrt{q})$.

Proof. The fact that $\{1, \alpha, \beta\}$ spans an ideal in $\mathbb{Q}[G]$, with structure constants as stated, follow from Theorem 3.6. For example when $q \equiv 1 \pmod{4}$ and $\varepsilon = (-1)^{\frac{q-1}{2}}$ in the notation of Theorem 3.6, we may write $\alpha^2 = m_0 + m_+\alpha + m_-\beta$ where m_0, m_+, m_- are positive integers expressing the number of ways to express 0 (respectively, each square, each nonsquare) as a sum of two squares in F . Here $m_0 = \frac{q-1}{2}$ is the number of solutions $0 = a + (-a)$ with $a \in S$; also $m_+ = \frac{q-5}{4}$ and $m_- = \frac{q-1}{4}$ by parts (i) and (iv) of Theorem 3.6.

Now let $\chi \in \widehat{G}$ be nontrivial. By Theorem 6.3(a), we have $\chi(\kappa) = 0$. If $q \equiv 1 \pmod{4}$ then

$$\chi(\alpha)^2 = \chi\left(\frac{q-1}{4}(1 + \kappa) - \alpha\right) = \frac{q-1}{4} - \chi(\alpha)$$

so that

$$\left(\chi(\alpha) + \frac{1}{2}\right)^2 = \frac{q}{4}$$

which yields $\chi(\alpha) = \frac{1}{2}(-1 \pm \sqrt{q})$; also $0 = \chi(\kappa) = \chi(1 + \alpha + \beta)$ gives $\chi(\beta) = \frac{1}{2}(-1 \mp \sqrt{q})$. If $q \equiv 3 \pmod{4}$ then

$$|\chi(\alpha)|^2 = \chi(\alpha)\overline{\chi(\alpha)} = \chi(\alpha\alpha^*) = \chi\left(\frac{q+1}{4} + \frac{q-3}{4}\kappa\right) = \frac{q+1}{4}$$

and so $|\chi(\alpha)| = \frac{1}{2}\sqrt{q+1}$. Also $0 = \chi(\kappa) = \chi(1 + \alpha + \beta) = 1 + \chi(\alpha) + \overline{\chi(\alpha)}$ so $\chi(\alpha) = \frac{1}{2}(-1 \pm i\sqrt{q})$ and $\chi(\beta) = \overline{\chi(\alpha)} = \frac{1}{2}(-1 \mp i\sqrt{q})$. \square

Exercises 7.

1. Consider the group algebra $R = F[G]$ of a finite (multiplicative) abelian group G over a field F , and let $\mathcal{A} \subseteq R$ be an ideal. Recall that R is an n -dimensional vector space with basis G , where $n = |G|$; and \mathcal{A} is a subspace. Assume that the characteristic of F does not divide n . (Thus $\text{char } F$ may equal zero; however $\text{char } F$ cannot equal p for any of the finitely many primes p dividing n .)
 - (a) Using linear algebra, explain why R has a subspace U complementary to \mathcal{A} , i.e. $R = \mathcal{A} \oplus U$; this means that $R = \mathcal{A} + U$ and $\mathcal{A} \cap U = 0$. Here you may cite any known theorems from linear algebra.
 - (b) Show by example that the subspace $U \leq R$ in (a) is not necessarily an ideal of R , or even a subalgebra, in general.
 - (c) Prove that there exists an F -linear transformation $P : R \rightarrow R$ such that $P^2 = P$, having image equal to \mathcal{A} and null space equal to U . (Again cite any known facts from linear algebra, using (a).)
 - (d) Define $T : R \rightarrow R$ by $T(v) = \frac{1}{n} \sum_{h \in G} h^{-1} P(hv)$. The hypothesis regarding $\text{char } F$ guarantees that n has an inverse in F (so we are not dividing by zero here). Prove that T is F -linear.
 - (e) Prove that $T(gv) = gT(v)$ for all $g \in G$ and $v \in R$.
 - (f) Prove that $T^2 = T$.
 - (g) Prove that $T(v) = v$ iff $v \in \mathcal{A}$.
 - (h) Prove that the image of T is \mathcal{A} , and the kernel of T is a subspace $\mathcal{B} \leq R$ complementary to \mathcal{A} ; so $R = \mathcal{A} \oplus \mathcal{B}$.
 - (i) Prove that $\mathcal{B} \subseteq R$ is in fact an ideal. (While (a) gives a complementary subspace, this is stronger: it gives a complementary ideal.)

Wherever well-known facts from linear algebra suffice, please indicate so. This is not the place to re-prove basic facts from linear algebra, only to demonstrate a knowledge of which facts these are. We remark that the assumption that G is abelian is not actually required here; however if G is nonabelian, we must speak of left ideals throughout, instead of (two-sided) ideals.

2. Let $R = F[G]$ where $F = \mathbb{F}_2$ and $G = \{1, g\}$ is cyclic. Note that the hypotheses of #1 are not satisfied. Here we show that the conclusion of #1 also fails. Find an ideal $\mathcal{A} \subseteq R$ for which there does not exist a complementary ideal; so there is no ideal $\mathcal{B} \subseteq R$ satisfying $R = \mathcal{A} \oplus \mathcal{B}$.

8. Difference Sets

Let G be a multiplicative group of order v . (While our groups will typically be abelian, we do not yet require this.) A (v, k, r) -**difference set in G** is a subset $D \subset G$ of size

$|D| = k$ such that every nonidentity element $g \in G$ is expressible in exactly r ways as $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. A necessary condition for the existence of such a difference set is the **feasibility relation** $(v-1)r = k(k-1)$, which follows by counting in two different ways the number of ordered pairs (d_1, d_2) of distinct elements of D . In order to avoid degenerate situations, we will always assume that $v > k$; that is, $k > r$ (which is easily seen to be equivalent, using the feasibility relation). We often call a difference set D **cyclic**, **abelian** or **nonabelian** according as G is cyclic, abelian or nonabelian. We refer to the triple of positive integers (v, k, r) as the **parameters** of the difference set; and the integer $n := k - r$ (soon to play a prominent role) is the **order** of D . Note that $n > 0$. Triples of integers (v, k, r) satisfying the feasibility conditions are not necessarily the parameters of any difference set, as we point out in the remarks preceding Theorem 8.2 below. The smallest feasible parameter set for which existence of a difference set is currently unknown, is apparently $(160, 54, 18)$.

We will reformulate the notion of difference sets in the language of group rings, which is ideally suited for this purpose. But first we need a little more terminology.

Given $\alpha = \sum_{g \in G} a_g g \in R[G]$ with $a_g \in R$, we denote $\alpha^* = \sum_{g \in G} a_g g^{-1} \in R[G]$. It is easy to see that the map $\alpha \mapsto \alpha^*$ is an **antiautomorphism** of $R[G]$, meaning that it is a bijective map satisfying

$$(\alpha + \beta)^* = \alpha^* + \beta^* \text{ and } (\alpha\beta)^* = \beta^*\alpha^*$$

for all $\alpha, \beta \in R[G]$. (If G is abelian, then clearly this map is an automorphism of the algebra.) In the following, we also denote $\kappa := \sum_{g \in G} g \in \mathbb{Z}[G]$.

Lemma 8.1. Let G be a multiplicative group of order v , and let $D \subset G$ be a subset of size $|D| = k$. Then D is a (v, k, r) -difference set iff

$$\delta\delta^* = n + r\kappa$$

where $\delta := \sum_{d \in D} d \in \mathbb{Z}[G]$ and $n := k - r$.

Proof. The relation $\delta\delta^* = n + r\kappa$ says that every nonidentity element $g \in G$ is expressible exactly r ways in the form $g = d_1 d_2^{-1}$ where $d_1, d_2 \in D$ with $d_1 \neq d_2$; and this is simply the requirement that D be a (v, k, r) -difference set. The identity element $1 \in G$ is expressible as $1 = dd^{-1}$ for each of the k elements $d \in D$; and this agrees with the constant term $n + r = k$ in the expression $n + r\kappa$. \square

A **symmetric (v, k, r) -design** is an incidence system $(\mathcal{P}, \mathcal{B})$ consisting of a set \mathcal{P} of cardinality $|\mathcal{P}| = v$ (whose elements are called **points**) and a collection \mathcal{B} consisting of v subsets of \mathcal{P} (called **blocks**) such that

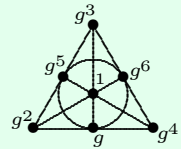
- (i) Each block contains exactly k points; and dually, each point lies in exactly k blocks.

- (ii) Any two distinct points lie in exactly r common blocks. Dually, any two distinct blocks intersect in exactly r points.

Again, a necessary condition for the existence of a symmetric (v, k, r) -design is the feasibility relation $(v-1)r = k(k-1)$, deduced by counting in two different ways the number of pairs of distinct points in a fixed block. As before, we call (v, k, r) the **parameters** of the design, and $n := k - r$ its **order**; and to avoid trivial cases, we always assume $v > k$, i.e. $k > r, n > 0$. From the feasibility relation, we see that any symmetric design with $r=1$ has parameters $(n^2+n+1, n+1, 1)$; this is called a **projective plane of order n** . Note that the feasibility relations are necessary, but not sufficient, condition for the existence of a symmetric design with a given set of parameters; for example, there is no symmetric design with the feasible parameter set $(43, 7, 1)$ (since there is no projective plane of order 6). Given this assertion and Theorem 8.2 below, it follows that there is also no $(43, 7, 1)$ -difference set. The smallest currently open parameter set for which the existence of a symmetric design has not yet been resolved, is $(81, 16, 3)$ (although so much is known about the automorphism group of a putative symmetric $(81, 16, 3)$ -design, that it cannot arise from any difference set).

Theorem 8.2. A (v, k, r) -difference set $D \subset G$ gives rise to a symmetric (v, k, r) -design whose point set is G and whose blocks are the right translates $Dh = \{dh : d \in D\}$, $h \in G$. This symmetric design admits G as a group of automorphisms permuting the points regularly (by right-multiplication).

Example 8.3: The Symmetric (7,3,1)- and (7,4,2)-Designs. Consider the cyclic group of order seven, $G = \{1, g, g^2, \dots, g^6\}$. The subset $D = \{g, g^2, g^4\}$ is a $(7, 3, 1)$ -difference set. The corresponding symmetric $(7, 3, 1)$ -design, whose seven translates are the lines shown on the right, is a projective plane of order 2. The complement of D is a $(7, 4, 2)$ -difference set $\{1, g^3, g^5, g^6\}$ whose translates are the seven quadrangles (sets of four points, no three collinear) in the same plane.



The $(7, 2, 1)$ -difference set generalizes in more than one way; see Exercises #3,4,5.

Proof of Theorem 8.2. Obviously each block Dh contains exactly k points dh , $d \in D$. Each point $g \in G$ lies in exactly k blocks $Dd^{-1}g$ for $d \in D$; this is because $g \in Dh$ iff $g = dh$ for some $d \in D$, iff $h = d^{-1}g$.

Given two distinct points $g_1 \neq g_2$ in G , a block Dh contains both points iff $(g_1, g_2) = (d_1h, d_2h)$ for some $d_1, d_2 \in D$, iff $d_1d_2^{-1} = g_1g_2^{-1}$ and $h = d_1^{-1}g_1$. There are exactly r pairs (d_1, d_2) in D satisfying these conditions; and each such pair (d_1, d_2) yields a unique block $Dh = Dd_1^{-1}g_1$. Thus there are exactly r blocks containing both points g_1 and g_2 . It remains only to show that any two distinct blocks intersect in exactly r points.

Let A be the $v \times v$ incidence matrix of our point-block structure: rows and columns of A are indexed by points and blocks respectively; and the entry in row $g \in G$ and column

Dh , $h \in G$, is 1 or 0 according as g is or is not in Dh . Let $J = J_v$ be the $v \times v$ matrix of 1's, and let $I = I_v$ be the $v \times v$ identity matrix. Using what we have already shown, $AJ = JA = kJ$ and $AA^T = nI + rJ$, where A^T is the transpose of A ; and of course also $A^TJ = JA^T = kI$. Since $n > 0$, clearly $nI + rJ$ is nonsingular (it has positive eigenvalues $n + rv$ and n of multiplicity 1 and $v - 1$ respectively, with eigenspaces $\langle \mathbf{1} \rangle$ and $\mathbf{1}^\perp$ respectively, where $\mathbf{1}$ is the all-ones vector of length v) and so A is also nonsingular. Since A and A^T both commute with I and J , they commute with each other; therefore $A^TA = nI + rJ$. This proves that any two distinct blocks intersect in exactly r points. \square

An **automorphism** of a design $(\mathcal{P}, \mathcal{B})$ is a transformation σ permuting the points, and also permuting the blocks, such that given any $P \in \mathcal{P}$ and $B \in \mathcal{B}$, we have $P \in B$ iff $\sigma(P) \in \sigma(B)$. Typically we identify each block with the set of its points; and in this view, an automorphism is the same thing as a permutation of the points such that for every $B \in \mathcal{B}$, its image $\sigma(B) := \{\sigma(P) : P \in B\}$ is also a block.

Theorem 8.4. Every automorphism of a symmetric (v, k, r) -design has the same number of fixed points as fixed blocks.

Proof. Let $(\mathcal{P}, \mathcal{B})$ be a symmetric design with $v \times v$ incidence matrix $A = (a_{P,B} : P \in \mathcal{P}, B \in \mathcal{B})$; here $a_{P,B} = 0$ or 1 according as $P \notin B$ or $P \in B$. Given an automorphism σ of $(\mathcal{P}, \mathcal{B})$, we construct $v \times v$ permutation matrices Π_1 and Π_2 representing the action of σ on points and blocks respectively. Thus for points P and P' , Π_1 has (P, P') -entry $\delta_{\sigma(P), P'} = 1$ or 0 according as $\sigma(P)$ is or is not equal to P' ; similarly Π_2 has (B, B') -entry $\delta_{\sigma(B), B'}$. Now $\Pi_1 A \Pi_2^T$ has (P, B) -entry equal to

$$\sum_{P', B'} \delta_{\sigma(P), P'} a_{P', B'} \delta_{\sigma(B), B'} = a_{\sigma(P), \sigma(B)} = a_{P, B}$$

since σ is an automorphism. This shows that $\Pi_1 A \Pi_2^T = A$. Now $\Pi_2^T = \Pi_2$ and A is invertible by the proof of Theorem 8.2; so $\Pi_1 = A \Pi_2 A^{-1}$. In particular, $\text{tr } \Pi_1 = \text{tr } \Pi_2$, which says that the number of points fixed by σ equals the number of blocks fixed by σ . \square

Not every symmetric design arises from a difference set; the designs constructed above are special in that they admit G as a regular group of automorphisms. Indeed, right-multiplication by an element $a \in G$ permutes points via $g \mapsto ga$ and blocks via $Dh \mapsto Dha$, thereby preserving incidence. To say that this group of automorphisms is **regular** is to say that for any two points g_1, g_2 , there is a unique automorphism in our group mapping $g_1 \mapsto g_2$ (in this case, right-multiplication by $a = g_1^{-1}g_2$). It is clear that this group of automorphisms of the design is isomorphic to the group G that we started with, and that it regularly permutes the blocks (as well as regularly permuting the blocks). In fact, for

a symmetric design, any group which regularly permutes the points must also regularly permute the blocks, although we do not prove this here.

Theorem 8.5. If D is a (v, k, r) -difference set in a group G , then the symmetric (v, k, r) -design constructed above admits a group of automorphisms isomorphic to G , regularly permuting both the points and the blocks.

Conversely, if $(\mathcal{P}, \mathcal{B})$ is a symmetric (v, k, r) -design with a group G of automorphisms regularly permuting both the points and the blocks, then there is a (v, k, r) -difference set $D \subset G$ which gives rise to the design $(\mathcal{P}, \mathcal{B})$.

Proof. We have only to prove the converse. Arbitrarily we choose a point and label it '1'. The other points are then labelled by the remaining group elements, using the regular action of G which we may assume acts by right-multiplication: element $g \in G$ maps point '1' to point ' g '. Choose a block B arbitrarily, and let D be the set of all points in B . Given our labelling of points by group elements, D is viewed as a subset of G , with $|D| = k$. Given $g \neq 1$ in G , by assumption there are exactly r blocks containing both the points g and 1. Any such block may be denoted Bh , or simply $Dh = \{dh : d \in D\}$, for some $h \in G$, using the regular action of G on the set of blocks; and we have $g, 1 \in Dh$ iff $(g, 1) = (d_1h, d_2h)$ for some $d_1, d_2 \in D$, iff $(g, h) = (d_1d_2^{-1}, d_2^{-1})$. Thus every non-identity element $g \in G$ is expressible as $g = d_1d_2^{-1}$ in exactly r ways. So $D \subset G$ is a (v, k, r) -difference set. \square

Theorem 8.6. Suppose that D is a (v, k, r) -difference set in a group G . Then so are the subsets

$$aDb := \{adb : d \in D\}; \quad D^* := \{d^{-1} : d \in D\}; \quad \text{and} \quad \sigma(D) := \{\sigma(d) : d \in D\}$$

for all $a, b \in G$, and every automorphism $\sigma \in \text{Aut } G$.

Proof. Let $\delta = \sum_{d \in D} d \in \mathbb{Z}[G]$ and $\kappa = \sum_{g \in G} g \in \mathbb{Z}[G]$ as before. By Lemma 8.1, $\delta\delta^* = n + r\kappa$. Given $a, b \in G$, the sum of the elements in aDb is $a\delta b$, which satisfies

$$(a\delta b)(a\delta b)^* = a\delta\delta^*a^{-1} = a(n + r\kappa)a^{-1} = n + r\kappa,$$

so aDb is also a (v, k, r) -difference set. It is also clear that $\sigma(D)$ is a (v, k, r) -difference set in G whenever $\sigma \in \text{Aut } G$.

It is clear from the definition that the dual of a symmetric (v, k, r) -design (in which the roles of points and blocks are reversed) is also a symmetric (v, k, r) -design (which may or may not be isomorphic to the original design). Moreover those symmetric designs arising from difference sets in the way we have shown, have a group G permuting both points and

blocks regularly. From a (v, k, r) -difference set $D \subset G$ we construct a symmetric (v, k, r) -design in which point P lies in block $d(B)$ iff $d \in D$, iff $d^{-1}(P)$ lies in the block B ; so in the dual design, the ‘point’ B lies in the ‘block’ $d^*(P)$ iff $d^* \in D^*$, where $D^* = \{d^{-1} : d \in D\}$. This dual design is also a symmetric (v, k, r) -design admitting G as a regular group of automorphisms; and so by Theorem 8.5, D^* is also a difference set. \square

Following Theorem 8.6, we usually consider two difference sets $D, D' \subset G$ to be **equivalent** if $D' = a\sigma(D)b$ for some $a, b \in G$ and $\sigma \in \text{Aut } G$, since it is in these cases the corresponding designs are isomorphic.

The search for difference sets in nonabelian groups is an interesting but very difficult problem. For the remainder of this section, *we will confine our attention to abelian groups*. If G is (multiplicative) abelian of order v , then for every integer t relatively prime to v , the map $g \mapsto g^t$ is an automorphism of G which extends to an automorphism of the group algebra: given $\alpha = \sum_{g \in G} a_g g \in \mathbb{Q}[G]$, $a_g \in \mathbb{Q}$, we define

$$\alpha^{[t]} = \sum_{g \in G} a_g g^t \in \mathbb{Q}[G].$$

Note that $(\alpha^{[s]})^{[t]} = \alpha^{[st]}$ and $\alpha^{[-1]} = \alpha^*$. Now if D is a (v, k, r) -difference set in an abelian group G , and t is relatively prime to v , it follows from Theorem 8.6 that the subset

$$D^{[t]} := \{d^t : d \in D\}$$

is also a (v, k, r) -difference set in G . However, $D^{[t]}$ may coincide with a translate gD for some $g \in G$. Hall’s Multiplier Theorem 8.9 indicates some sufficient conditions for this to occur. But first we prove

Theorem 8.7. Let G be a multiplicative cyclic group of order v , and consider a nonempty subset $D \subset G$ of size $|D| = k < v$ with sum $\delta = \sum_{d \in D} d \in \mathbb{Z}[G]$. Then

(a) D is a (v, k, r) -difference set in G iff $k^2 - rv = n := k - r$ and

$$|\chi(\delta)| = \sqrt{n}$$

for every nontrivial $\chi \in \widehat{G}$.

(b) Assuming G is cyclic, in (a) it suffices to verify $|\chi_d(\delta)| = \sqrt{n}$ for a set of representatives χ_d of the characters of order d , where d ranges over the divisors of v with $d > 1$.

Proof. By Lemma 8.1, D is a (v, k, r) -difference set iff $\delta\delta^* = n + r\kappa$. By Corollary 7.3, this is equivalent to

$$(8.8) \quad |\chi_d(\delta)|^2 = \chi_d(\delta)\overline{\chi_d(\delta)} = \chi_d(\delta\delta^*) = \chi_d(n + r\kappa) = n + r\chi_d(\kappa)$$

for all $d \mid n$. For $d=1$ this gives another proof of $k^2 = n + rv$, which is just the feasibility relation. For $d > 1$, we have $\chi_d(\kappa) = \sum_{g \in G} \chi_d(g) = 0$ by Theorem 6.3(a), so (8.8) reduces to $|\chi_d(\delta)|^2 = n$. \square

Theorem 8.9 (Hall's Multiplier Theorem [Ha], [HR]). Let D be a (v, k, r) -difference set in an abelian group G of order v . Suppose that the order $n = k - r$ has a prime divisor $p > r$ which does not divide v . Then $D^{[p]} = gD$ for some $g \in G$.

Proof. Let $\delta = \sum_{d \in D} d$ and $\kappa = \sum_{g \in G} g$, so that $\delta\delta^{[-1]} = n + r\kappa$. We see from the Multinomial Theorem that $\delta^p = \delta^{[p]} + p\alpha$ for some $\alpha \in \mathbb{Z}[G]$, so

$$\delta^{[p]}\delta^{[-1]} = \delta^p\delta^{[-1]} - p\alpha\delta^{[-1]} = \delta^{p-1}\delta\delta^{[-1]} + p\alpha_1 = (n + r\kappa)\delta^{p-1} + p\alpha_1 = r\kappa + p\alpha_2$$

for some $\alpha_1, \alpha_2 \in \mathbb{Z}[G]$. Since all coefficients on the left side are non-negative integers, this must also be true on the right side; and since $p > r$ this means that all coefficients in α_2 are non-negative integers. Multiplying both sides by κ yields $k^2\kappa = rv\kappa + p\alpha_2\kappa$; and using the feasibility relation $k^2 = n + rv$ we obtain $p\alpha_2\kappa = n\kappa$. Applying $[-1]$ yields also $p\alpha_2^{[-1]}\kappa = n\kappa$. Now

$$\begin{aligned} (\delta^{[p]}\delta^{[-1]})(\delta^{[p]}\delta^{[-1]})^{[-1]} &= \delta^{[p]}\delta^{[-1]}\delta^{[-p]}\delta = (\delta\delta^{[-1]})(\delta\delta^{[-1]})^{[p]} = (n+r\kappa)(n+r\kappa)^{[p]} \\ &= n^2 + 2rn\kappa + r^2v\kappa. \end{aligned}$$

On the other hand,

$$(\delta^{[p]}\delta^{[-1]})(\delta^{[p]}\delta^{[-1]})^{[-1]} = (r\kappa + p\alpha_2)(r\kappa + p\alpha_2^{[-1]}) = r^2v\kappa + 2rn\kappa + p^2\alpha_2\alpha_2^{[-1]}.$$

Equating these two expressions yields

$$p^2\alpha_2\alpha_2^{[-1]} = n^2.$$

The expansion $\alpha_2 = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$ must have exactly one nonzero coefficient a_g since the coefficients are non-negative integers and the right side has a single term n^2 . It follows that $p\alpha_2 = ng$ for some $g \in G$. We arrive at

$$\delta^{[p]}\delta^{[-1]} = ng + r\kappa = \delta\delta^{[-1]}g.$$

We would like to cancel $\delta^{[-1]}$ from both sides, but first we need to know that $\delta^{[-1]}$ is not a zero divisor in $\mathbb{Q}[G]$. The latter relation takes the form $\rho\delta^{[-1]} = 0$ where $\rho = \delta^{[p]} - \delta g \in \mathbb{Q}[G]$. Now each $\chi \in \widehat{G}$ satisfies

$$\chi(\rho)\chi(\delta^{[-1]}) = \chi(\rho\delta^{[-1]}) = \chi(0) = 0.$$

For the trivial character, we have $\chi(\delta^{[-1]}) = k$; and by Theorem 8.6, $D^{[-1]}$ is a (v, k, r) -difference set, so $|\chi(\delta^{[-1]})| = \sqrt{v}$ by Theorem 8.7. In either case, $\chi(\delta^{[-1]}) \neq 0$, so $\chi(\rho) = 0$ for all $\chi \in \widehat{G}$. By Corollary 7.3(a), $\rho = \delta^{[p]} - \delta^g = 0$ as required. \square

Given a difference set D in an abelian group G , a **multiplier** of D is an automorphism $[t] \in \text{Aut } G$ (where t is an integer relatively prime to $v = |G|$) such that $D^{[t]} = Dg$ for some $g \in G$. It is not hard to see that the product of two multipliers of D is again a multiplier of D ; and so the set of multipliers forms the **multiplier group** of D . Hall's Multiplier Theorem shows that this group contains all primes $p > r$ which divide n but do not divide v . (It has long been conjectured that the hypothesis $p > r$ should not be necessary for the stated conclusion; but despite much work on this nagging problem, this **Multiplier Conjecture** remains open.)

Theorem 8.10. Let D be a (v, k, r) -difference set in an abelian group G of order v . Let $[t] \in \text{Aut } G$ be a multiplier of D . Then there exists a translate Dh ($h \in G$) which is fixed by $[t]$, i.e. $(Dh)^{[t]} = Dh$.

The point is that Dh generates the same symmetric design as D , since these two difference sets have the same translates in G ; so for most purposes, we may assume $[t]$ fixes D itself, otherwise replace D by an appropriate translate.

Proof of Theorem 8.10. The automorphism $[t] \in \text{Aut } G$ acts as an automorphism of the associated symmetric design, since $g \in Dh$ iff $g^t \in (Dh)^{[t]}$. Since $1^t = 1$, $[t]$ fixes at least one point; so by Theorem 8.4, $[t]$ has at least one fixed block Dh , $h \in G$. \square

Example 8.11: Constructions using Multipliers. Consider the cyclic group $G = \{1, g, g^2, \dots, g^6\}$ of order seven. Although it is not hard to find difference sets of order 2 in G (see Example 8.3), Hall's Multiplier Theorem makes the job even faster. The prime $p = 2$ divides $n = 2$ but not $v = 7$, so $[2] \in \text{Aut } G$ is a multiplier. By Theorem 8.10, any difference set is equivalent to one invariant under the multiplier. Now $[2]$ has three orbits on G : $\{1\}$, $\{g, g^2, g^4\}$, $\{g^3, g^5, g^6\}$. In order that $D^{[2]} = D$, D must be a union of these orbits. We obtain $D = \{g, g^2, g^4\}$ and $D^* = \{g^3, g^5, g^6\}$ as $(7, 2, 1)$ -difference sets; every $(7, 2, 1)$ -difference set is therefore a translate of one of these. Taking their unions with the orbit $\{1\}$ gives two $(7, 4, 2)$ -difference sets; and every difference set with these parameters is a translate of one of these.

Now consider the cyclic group $G = \{1, g, g^2, g^{20}\}$ of order 21. A cyclic $(21, 5, 1)$ -difference set in G has order 4 and so must have $[2]$ as a multiplier. The orbits of $[2]$ on G are $\{1\}$, $\{g^7, g^{14}\}$, $\{g^3, g^6, g^{12}\}$, $\{g^9, g^{15}, g^{18}\}$, $\{g, g^2, g^4, g^8, g^{11}, g^{16}\}$ and $\{g^5, g^{10}, g^{13}, g^{17}, g^{19}, g^{20}\}$; and any $(21, 5, 1)$ -difference set D is (up to translation) a union of cosets. Since $k = 5$, we must have $D = \{g^3, g^6, g^7, g^{12}, g^{14}\}$ or $\{g^7, g^9, g^{14}, g^{15}, g^{18}\}$. It is not hard to check that both of these are in fact difference sets; and they have the form D and D^* , so the corresponding designs are dual to each other.

Example 8.12: Nonexistence via Multipliers. We show that there is no cyclic projective plane of order 10. Such a design would necessarily arise from a $(111, 11, 1)$ -difference set D in a cyclic group G of order 111. The plane has order 10 and so $[2]$ is a multiplier. Without loss of generality, $D^{[2]} = D$. A short computer program helps to enumerate the orbits of $[2]$ on G , which are $\{1\}$, $\{g^{37}, g^{74}\}$, S , g^3S and $g^{11}S$ where $|S| = 36$. Since there is no union of orbits having combined size $k = 11$, there can be no such difference set. (There is in fact no projective plane of order 10, as we now know by extensive computer search. It is remarkable how much easier it is to prove nonexistence in the cyclic case.)

Example 8.13: Nonexistence via Characters. We prove that there is no $(154, 18, 2)$ -difference set in a cyclic group G . Here the order is $n = 18 - 2 = 16$. We expect $[2]$ to be a multiplier, but we cannot use Theorem 8.9 as stated since $p = 2$ does not exceed $r = 2$. But suppose $D \subset G$ is a $(154, 18, 2)$ -difference set, and let $\chi \in \widehat{G}$ be a character of order 11. The values of χ are in $\mathcal{O} := \mathbb{Z}[\zeta]$, $\zeta = \zeta_{11}$. By Theorem 8.7, $\delta := \sum D$ satisfies $|\chi(\delta)|^2 = 16$. Denoting the principal ideal $\mathcal{A} = (\chi(\delta)) \subset \mathcal{O}$, this yields the factorization $\mathcal{A}\overline{\mathcal{A}} = (2)^4$ and so $\mathcal{A} = \overline{\mathcal{A}} = (2)^2$. Now the ideal $(2) = 2\mathcal{O} \subset \mathcal{O}$ is prime since the quotient $\mathcal{O}/(2) \cong \mathbb{Z}[x]/(2, \Phi_{11}(x)) \cong \mathbb{F}_2[x]/(\Phi_{11}(x)) \cong \mathbb{F}_{2^{10}}$ is a field. (Any root of $\Phi_{11}(x)$ in an extension of \mathbb{F}_2 is a primitive 11-th root of unity; and any extension \mathbb{F}_{2^k} having such a root must have $11 \mid 2^k - 1$, and this requires $10 \mid k$.) Since $\mathcal{A} = (\chi(\delta)) = (4)$, we must have $\chi(\delta) = 4u$ for some unit $u \in \mathcal{O}^\times$. But every automorphism $\sigma \in \text{Aut } \mathbb{Q}[\zeta]$ has the property that $\sigma \circ \chi : G \rightarrow \mathbb{Q}[\zeta]$ is also a nontrivial character, so the same reasoning gives $|\sigma(\chi(\delta))| = 4$. Thus $u \in \mathcal{O}$ satisfies $|\sigma(u)| = 1$ for every $\sigma \in \text{Aut } \mathbb{Q}[\zeta]$. By Theorem 4.10, u is a root of unity in $\mathbb{Q}[\zeta_{11}]$; so $u = \pm \zeta^k$ and $\chi(\delta) = \pm 4\zeta^k$ for some $k \in \{0, 1, 2, \dots, 10\}$. However $[G : H] = 11$ where $H = \ker \chi = \{g \in G : \chi(g) = 1\}$ and so $G = H \cup Ht \cup Ht^2 \cup \dots \cup Ht^{10}$ where $t \in G$ has order 11 satisfying $\chi(t) = \zeta$; thus $\chi(\delta) = a_0 + a_1\zeta + a_2\zeta^2 + \dots + a_{10}\zeta^{10}$ where $a_i = |D \cap Ht^i|$. Since $\Phi_{11}(x) = 1 + x + x^2 + \dots + x^{10}$ is the minimal polynomial of ζ over \mathbb{Q} , these two expressions for $\chi(\delta)$ can only agree if $a_0 + a_1x + a_2x^2 + \dots + a_{10}x^{10} = \pm 4x^k + a\Phi_{11}(x)$ for some $a \in \mathbb{Q}$. Comparing coefficients gives $a \in \mathbb{Z}$ and $154 = \sum_{i=0}^{10} a_i = \pm 4 + 11a$ and $154 \equiv \pm 4 \pmod{11}$, a contradiction. Thus no $(154, 18, 2)$ -difference set can exist over a cyclic group.

We remark on the necessity of observing that the ideal $(2) \subset \mathcal{O}$ is prime; if this were not the case, then possibly $(2) = \mathfrak{P}\overline{\mathfrak{P}}$ for some ideal $\mathfrak{P} \subset \mathcal{O}$ such that $(\chi(\delta)) = \mathfrak{P}^2$ and $(\overline{\chi(\delta)}) = \overline{\mathfrak{P}}^2$, which would have invalidated our argument.

The literature on difference sets is vast and growing quickly; see for example the surveys [Ju], [JS1], [JS2] on this subject. From the extensive list of known constructions and general nonexistence results, we have highlighted only a few above, with a preference for techniques using cyclotomic fields and group characters. It is with this preference in mind that we have we have passed over many important results, in particular

Theorem 8.14 (Bruck, Ryser, Chowla [BR], [CR]). Suppose there exists a symmetric (v, k, r) -design of order $n := k - r$. If v is even, then n is a square. If v is odd, then the Diophantine equation $nx^2 + (-1)^{\frac{v-1}{2}}y^2 = z^2$ has a nontrivial integer solution (i.e. $(x, y, z) \neq (0, 0, 0)$).

While this condition does not rule out the designs of Examples 8.12 and 8.13, it does rule out many others, including the projective plane of order 6 mentioned earlier. Of course every parameter set (v, k, r) for which no symmetric design exists, means also that there is no difference set with the given parameters.

Exercises 8.

1. Let G be a cyclic group of order seven. How many $(7, 3, 1)$ -difference sets does G have? If D is one such difference set, are all the others of the form aDb or $(aDb)^*$ using Theorem 8.6?
2. Generalizing Example 8.3, show that if $(\mathcal{P}, \mathcal{B})$ is a symmetric (v, k, r) -design, then by complementing every block $B \in \mathcal{B}$ we get a family of subsets $\mathcal{B}' = \{\mathcal{P} \setminus B : B \in \mathcal{B}\}$ such that $(\mathcal{P}, \mathcal{B}')$ is also a symmetric design. Find the parameters of $(\mathcal{P}, \mathcal{B}')$; and show that the **complementary design** $(\mathcal{P}, \mathcal{B}')$ has the same order as the original design $(\mathcal{P}, \mathcal{B})$. (Note that in view of Theorem 8.5, every difference set $D \subset G$ must also yield a **complementary difference set** $D' := G \setminus D$ of the same order.)
3. Let G be an *additive* (rather than multiplicative) group of order v . Then a **(v, k, r) -difference set** in G is a subset $D \subset G$ of size $|D| = k < v$ such that every nonzero element $g \in G$ can be expressed as $g = d_1 - d_2$ in exactly r ways. Each integer t relatively prime to v determines an automorphism $[t] \in \text{Aut } G$, $g \mapsto tg$; and such a map is a **multiplier** of D if $tD = D + g$ for some $g \in G$.
 - (a) Let G be the additive group of a finite field \mathbb{F}_q , $q \equiv 3 \pmod{4}$; and let D be the set of nonzero squares in \mathbb{F}_q . Show that D is a difference set in G , and determine its parameters. This construction gives the **Paley difference sets**; it includes the $(7, 3, 1)$ -difference set of Example 8.3 as a special case.
 - (b) Find all multipliers of the difference set D in (a). In the strict sense that we have defined multipliers $[t]$, we have only considered $t \in \mathbb{Z}$. Can you generalize the definition of multipliers to include more general automorphisms?
4. Let V be a vector space of dimension $e \geq 3$ over a finite field $F = \mathbb{F}_q$. Let \mathcal{P} be the set of all 1-dimensional subspaces of V , and let \mathcal{B} be the set of all $(e-1)$ -dimensional subspaces of V .
 - (a) Show that $|\mathcal{P}| = |\mathcal{B}| = \frac{q^e - 1}{q - 1}$.
 - (b) For $P \in \mathcal{P}$ and $B \in \mathcal{B}$, we say that P lies in B if P is a subspace of B . Show that this defines a symmetric (v, k, r) -design where $v = \frac{q^e - 1}{q - 1}$. Express k , r and $n := k - r$ in terms of q and e .
 - (c) Show that when $e = 3$, the design $(\mathcal{P}, \mathcal{B})$ is a projective plane of order n . These are in fact the **classical projective planes**, again including Example 8.3 as a special case.
5. Let $E \supset F$ be an extension of finite fields of degree $e \geq 3$ where $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^e}$. Let $\omega \in E$ be a generator of the cyclic group E^\times , i.e. a primitive $(q^e - 1)$ -st root of unity.
 - (a) Show that ω^v is a generator of the multiplicative group F^\times , where $v = \frac{q^e - 1}{q - 1}$; that is, ω^v is a primitive $(q - 1)$ -st root of unity.
 - (b) Consider the quotient group $G = E^\times / F^\times$, a cyclic group of order $v = \frac{q^e - 1}{q - 1}$. Note that for each $\alpha \in E^\times$ and $a \in F^\times$, we have $\text{Tr}_{E/F}(a\alpha) = 0$ iff $\text{Tr}_{E/F}(\alpha) = 0$ (using the F -linearity of the trace map); so we have a well-defined subset $D \subset G$ consisting of all cosets αF^\times , $\alpha \in E^\times$ such that $\text{Tr}_{E/F} \alpha = 0$. Show that D is a cyclic difference set in G having the same parameters as the design in #4. (These are the **Singer designs**.)

9. Hadamard Matrices

A **Hadamard matrix** of order $m \geq 1$ is an $m \times m$ matrix H with entries ± 1 satisfying $HH^T = mI$. Examples of the smallest Hadamard matrices, having orders 1, 2, 4, 8, are

$$(9.1) \quad [+], \quad \begin{bmatrix} + & + \\ + & - \end{bmatrix}, \quad \begin{bmatrix} - & + & + & + \\ + & - & + & + \\ + & + & - & + \\ + & + & + & - \end{bmatrix}, \quad \begin{bmatrix} + & + & + & + & + & + & + & + \\ - & + & + & + & - & + & - & - \\ - & - & + & + & + & - & + & - \\ - & - & - & + & + & + & - & + \\ - & + & - & - & + & + & + & - \\ - & - & + & - & - & + & + & + \\ - & + & - & + & - & - & + & + \\ - & + & + & - & + & - & - & + \end{bmatrix}$$

where we abbreviate ± 1 by \pm .

Theorem 9.2. The order m of any Hadamard matrix satisfies $m = 1, 2$ or $4n$ for some $n \geq 1$.

Proof. Let H be a Hadamard matrix of order $m > 2$, and let $u, v, w \in \{\pm 1\}^n$ be its first three rows. Since the vectors $u+v$ and $u+w$ have even entries, $m = u \cdot u = (u+v) \cdot (u+w) \equiv 0 \pmod{4}$. \square

It is not known whether the converse of Theorem 9.2 holds; but it is a popular conjecture that for every positive $m \equiv 0 \pmod{4}$, there is a Hadamard matrix of order m . The smallest currently open case is $m = 668$. How should one go about trying to construct a Hadamard matrix of such a size? Whatever is the best way, certainly the worst way is to hope to go through all 2^{m^2} matrices of size $m \times m$ with entries ± 1 until finding success. In trying to convey to my non-mathematical friends a sense of the kind of problems combinatorialists work on, I will often describe the search for a Hadamard matrix of size 668; but the magnitude of such a search typically fails to impress my friends who are unaware that if all the computers in the world were dedicated to a naive search of 2^{668^2} cases at the optimistic rate of a million cases per second, it would still take *much more than* 10^{100000} times the current age of the universe to finish the task.

Rather than not looking at all, we look where the chances seem better. We are reminded of the old story (often called **The Streetlight Effect**), one version [Ho] of which goes:

A man got drunk in Memphis one night. Staggering down the street, he stumbled into an alley. His watch fell out of his pocket. He heard it fall. He got up, and walked on down to the corner. There he got down on his hands and knees and started crawling all around under the electric light. Soon the traffic was blocked. A police officer came up to him and said : "What're you doing? Can't you see you're blocking traffic?" The drunk replied: "Well, I losht mer watch. It was my daddy's watch; sort of an heirloom in the family, and I've juss gotta find that watch."

The cop said: “All right, boss, I’ll help you find it. Where did you lose it?” The drunk: “I losht it up there in that damn dark alley.” The cop: “Well, why don’t you look for it down there where you lost it?” The drunk: “Why, you big fat fool, can’t you see there’s a lot more light up here?”

The story offers us some guiding principles, both in looking for examples, and in trying to glean insight from the known examples directing us what theorems we should be trying to prove (at least whether existence or nonexistence results). When hunting for examples, we are wise to look where the light is best, provided we look where our chances are good. But before ruling out the darker regions or investing too much time trying to prove nonexistence there, consider that the lack of known examples in the darker regions is due to the difficulty of finding them there. (It is usually this second lesson that is intended by ‘the streetlight effect’.)

The literature on Hadamard matrices is far too vast to adequately summarize here, so we will content ourselves with describing a few general types of construction and some approaches to classifying or proving nonexistence in special cases. Cyclotomic integers play a key role in both of these ventures, but particularly in proving nonexistence or classification results; however much of the work constructing examples uses group rings and representations where cyclotomic integers arise in a somewhat clerical way.

However before describing general types of construction, we should note that if H is a Hadamard matrix of order m , then $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H = \begin{bmatrix} H & H \\ H & -H \end{bmatrix}$ is a Hadamard matrix of order $2m$. So for the existence problem, it suffices to consider only orders $m \equiv 4 \pmod{8}$, i.e. $m = 4n$ where n is odd; and we will often confine our attention to this case. The doubling trick we have just mentioned is a special case of

Theorem 9.3. If H_i is a Hadamard matrix of order m_i for $i \in \{1, 2\}$, then $H_1 \otimes H_2$ is a Hadamard matrix of order $m_1 m_2$.

Proof. Each entry in $H_1 \otimes H_2$ is the product of an entry in H_1 times an entry in H_2 , hence equal to ± 1 . Also $(H_1 \otimes H_2)(H_1 \otimes H_2)^T = (H_1 H_1^T) \otimes (H_2 H_2^T) = m_1 I_{n_1} \otimes m_2 I_{m_2} = m_1 m_2 I_{m_1 m_2}$. \square

We also mention that if H is Hadamard, then multiplying some of the rows of H by -1 , and multiplying some of the columns by -1 , then permuting rows and permuting columns, results in another Hadamard matrix which is said to be **monomially equivalent** to H . Since H^T is also Hadamard, one might also consider the coarser equivalence relation which allows for transposing of Hadamard matrices. In counting Hadamard matrices, we may be interested in the raw number of Hadamard matrices of order m (a rapidly growing function of m), or in the number of equivalence classes of Hadamard matrices of order m (either up to monomial equivalence, or up to monomial equivalence and transpose). The exact number of monomial equivalence classes of Hadamard matrices of order m is known only for $m \leq 32$. For $m = 4, 8, 12, 16, 20, 24, 28, 32$, the number of classes is 1, 1, 1, 5, 3, 60, 487, 13710027.

Skew-Type Hadamard Matrices

A Hadamard matrix of order m is of **skew type** if it has the form $I_m + S$ where S is $m \times m$ skew-symmetric with entries ± 1 off its main diagonal. The fourth example in (9.1) is of this type. After scaling certain rows and columns by -1 , one shows that every skew-type Hadamard matrix takes the equivalent form

$$H = \begin{bmatrix} + & + & + & \cdots & + \\ - & & & & \\ - & & I+A & & \\ \vdots & & & & \\ - & & & & \end{bmatrix}$$

where

$$(9.4) \quad A \text{ is skew symmetric } (A^T = -A) \text{ of size } (m-1) \times (m-1) \text{ with zeroes on its main diagonal and entries } \pm 1 \text{ elsewhere; and}$$

$$(9.5) \quad AJ = JA = 0 \text{ and } A^2 = J - (m-1)I \text{ where } I = I_{m-1} \text{ and } J = J_{m-1} \text{ are the identity matrix and all-ones matrix of size } (m-1) \times (m-1) \text{ respectively.}$$

These conditions are equivalent to the assertion that $A = A_1 - A_1^T$ where A_1 is the $(0, 1)$ -incidence matrix of a symmetric $(4n-1, 2n-1, n-1)$ -design (and A_1^T is the incidence matrix of the dual design with the same parameters). Such a design has order n and is called a **Hadamard 2-design**. Of course any $(4n-1, 2n-1, n-1)$ -difference set in an abelian group of order $v = 4n-1$ immediately gives such a design and Hadamard matrix of order $4n$. These difference sets are usually said to be of **Paley type**. But there is conflicting terminology: some authors, a minority it seems, refer to $(4n-1, 2n-1, n-1)$ -difference sets as *Hadamard difference sets*. Others reserve this terminology for the parameters $(4n^2, 2n^2 \pm n, n^2 \pm n)$ discussed below.

The classical construction, due to Paley, uses the additive group of \mathbb{F}_q , $q \equiv 3 \pmod{4}$, in which the squares form a $(4n-1, 2n-1, n-1)$ difference set where $n = \frac{1}{4}(q+1)$; see Exercise #8.3. After rewriting the group as a multiplicative group G of order q , we let $\alpha, \beta, \kappa \in \mathbb{Z}[G]$ be the elements denoted by

$$\alpha = \sum_{g \in S} g, \quad \beta = \sum_{g \in N} g, \quad \kappa = \sum_{g \in G} g.$$

Note that $\kappa = 1 + \alpha + \beta$ (where the '1' represents $0 \in \mathbb{F}_q$, but rewritten multiplicatively). Now Theorem 7.7(b) yields $\alpha\alpha^* = n + (n-1)\kappa$. This expresses the fact that the squares form a difference set with the indicated parameters. When $q = 7$, this gives the Hadamard matrix of order 8 listed in (9.1).

To show that there exist also nonclassical skew-type Hadamard matrices, we present next the **twin prime power construction** [SS] using a Paley-type difference set of order $n = \frac{1}{4}(q+1)^2$ whenever both q and $q+2$ are odd prime powers. Here G is the additive

group of the ring $R := \mathbb{F}_q \oplus \mathbb{F}_{q+2}$. The difference set D consists of pairs $(a, b) \in R$ such that

- a and b are both nonzero squares in their respective fields; or
- a and b are both nonsquares in their respective fields; or
- $a \in \mathbb{F}_q$ is arbitrary and $b = 0$.

Note that $|G| = q(q+2) = 4n-1$ and $|D| = \frac{1}{4}(q^2-1) + \frac{1}{4}(q^2-1) + q = 2n-1$. We write $G = G_1 \times G_2$ and

$$\kappa = \sum_{g \in G} = \kappa_1 \kappa_2 \in \mathbb{Q}[G] \quad \text{where } \kappa_i = \sum_{g \in G_i} g \in \mathbb{Q}[G_i];$$

see the description of group algebras for direct product groups in Section 7. We also let $\alpha_i, \beta_i \in \mathbb{Q}[G_i]$ corresponding to nonzero squares and nonsquares in the respective fields, so that $\kappa_i = 1 + \alpha_i + \beta_i$ in the notation of Theorem 7.7. Now $\delta = \sum_{d \in D} d = \alpha_1 \alpha_2 + \beta_1 \beta_2 + \kappa_1$. To verify that D is a $(4n-1, 2n-1, n-1)$ -difference set in G , i.e. $\delta \delta^* = n + (n-1)\kappa$, it suffices by Theorem 8.7 to check that $|\chi(\delta)| = \sqrt{n}$ for every nontrivial $\chi \in \widehat{G}$. Recall that $\chi = \chi_1 \times \chi_2$ where $\chi_i \in \widehat{G_i}$, and at least one of χ_1, χ_2 is nontrivial. Again by the comments of Section 7,

$$\chi(\delta) = \chi_1(\alpha_1)\chi_2(\alpha_2) + \chi_1(\beta_1)\chi_2(\beta_2) + \chi_1(\kappa_1).$$

If χ_1 is trivial, then χ_2 is nontrivial and

$$\chi(\delta) = \frac{q-1}{2}\chi_2(\alpha_2) + \frac{q-1}{2}\chi_2(\beta_2) + q = \frac{q-1}{2}(-1) + q = \frac{q+1}{2} = \sqrt{n}.$$

If χ_2 is trivial then χ_1 is nontrivial and

$$\chi(\delta) = \chi_1(\alpha_1)\frac{q+1}{2} + \chi_1(\beta_1)\frac{q+1}{2} = (-1)\frac{q+1}{2} = -\sqrt{n}.$$

In the remaining case, both χ_1 and χ_2 are nontrivial and

$$\begin{aligned} \chi_1(\alpha_1) &= \frac{1}{2}(-1 + \varepsilon_1\sqrt{q}), & \chi_1(\beta_1) &= \frac{1}{2}(-1 - \varepsilon_1\sqrt{q}), \\ \chi_2(\alpha_2) &= \frac{1}{2}(-1 + \varepsilon_2\sqrt{q+2}), & \chi_2(\beta_2) &= \frac{1}{2}(-1 - \varepsilon_2\sqrt{q+2}) \end{aligned}$$

where $\varepsilon_1 \in \{1, -1\}$ and $\varepsilon_2 \in \{i, -i\}$ if $q \equiv 1 \pmod{4}$; or $\varepsilon_1 \in \{i, -i\}$ and $\varepsilon_2 \in \{1, -1\}$ if $q \equiv 3 \pmod{4}$. Now

$$\chi(\delta) = \chi_1(\alpha_1)\chi_2(\alpha_2) + \chi_1(\beta_1)\chi_2(\beta_2) = \frac{1}{2}(1 + \varepsilon_1\varepsilon_2\sqrt{q(q+2)}) = \frac{1}{2}(1 \pm i\sqrt{q(q+2)})$$

and $|\chi(\delta)|^2 = \frac{1}{4}(1 + q(q+2)) = \frac{1}{4}(q+1)^2 = n^2$.

Williamson-Hadamard Matrices

A Hadamard matrix of order $m = 4n$ is of **Williamson type** if it has the form

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

where A, B, C, D are symmetric circulant matrices of order n which commute with each other. We recall that an $n \times n$ matrix is **circulant** if each row is a cyclic shift of the

previous row, with ‘wraparound’. More precisely, the set of all $n \times n$ circulant matrices is the algebra $\mathbb{Q}[T]$ generated by the $n \times n$ matrix

$$T = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Note that $\{I, T, T^2, \dots, T^{n-1}\}$ is a basis for $\mathbb{Q}[T]$. For reasons described already, we will assume $n = 2t+1$ is odd. We have required A, B, C, D to be symmetric circulant matrices; equivalently, they lie in the subalgebra of $\mathbb{Q}[T]$ having basis $\{I\} \cup \{T^i + T^{-i} : 1 \leq i \leq t\}$. Now the condition $HH^T = mI_m$ reduces to the single relation

$$A^2 + B^2 + C^2 + D^2 = 4nI_n.$$

In the following, the group $G = \{1, g, g^2, \dots, g^{n-1}\}$ is cyclic of order n ; and we abbreviate the elements $\omega_i = g^i + g^{-i} \in \mathbb{Z}[G]$ for $i \in \mathbb{Z}/n\mathbb{Z}$ which are easily seen to satisfy $\omega_i \omega_j = \omega_{i+j} + \omega_{i-j}$ (noting that all indices here are modulo n). As before, we write $\kappa = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} g^i = 1 + \sum_{i=1}^t \omega_i \in \mathbb{Z}[G]$ where $t = \frac{n-1}{2}$.

Theorem 9.6 ([Wi]; see also [BH]). Let G be a cyclic group of order $n = 2t + 1$. The following conditions are equivalent.

- (i) There exists a Hadamard matrix of order $m = 4n = 8t + 4$ of Williamson type.
- (ii) There exist elements $\alpha, \beta, \gamma, \delta \in \mathbb{Z}[G]$ of the form

$$\alpha = 1 + \sum_{i=1}^t a_i \omega_i, \quad \beta = 1 + \sum_{i=1}^t b_i \omega_i, \quad \gamma = 1 + \sum_{i=1}^t c_i \omega_i, \quad \delta = 1 + \sum_{i=1}^t d_i \omega_i$$

where $a_i, b_i, c_i, d_i \in \{1, -1\}$, satisfying

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 4n.$$

- (iii) There exists a partition $\{1, 2, \dots, t\} = I_1 \sqcup I_2 \sqcup I_3 \sqcup I_4$ (with I_j possibly empty) and signs $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_t \in \{1, -1\}$ such that the elements

$$\tau_j = 1 + 2 \sum_{i \in I_j} \varepsilon_i \omega_i \in \mathbb{Z}[G]$$

satisfy $\tau_1^2 + \tau_2^2 + \tau_3^2 + \tau_4^2 = 4n$.

Proof. It is easily verified that for an $m \times m$ matrix H of the form described above, one has $HH^T = mI_m$ iff $A^2 + B^2 + C^2 + D^2 = 4nI_n$; here we use the fact that A, B, C, D are commuting symmetric $n \times n$ matrices with entries ± 1 . This condition requires that

$$A = a_0I + \sum_{i=1}^t a_i(T^i + T^{-i}), \quad \dots, \quad D = d_0I + \sum_{i=1}^t d_i(T^i + T^{-i})$$

where all coefficients $a_i, b_i, c_i, d_i \in \{1, -1\}$. Without loss of generality, $a_0 = 1$; otherwise replace A by $-A$ while preserving all necessary conditions. Similarly, $b_0 = c_0 = d_0 = 1$. The algebra $\mathbb{Q}[T]$ is nothing other than the group algebra of a cyclic group G of order n ; and using the generic symbol g for the generator of G , the isomorphism takes the form $\mathbb{Q}[T] \rightarrow \mathbb{Q}[G]$, $\sum_{i=0}^{n-1} a_i T^i \mapsto \sum_{i=0}^{n-1} a_i g^i$. Taken together, these facts establish the equivalence of (i) and (ii).

Now given $\alpha, \beta, \gamma, \delta$ as in (ii), let us write $\alpha = 2\alpha_0 - \kappa$ where $\alpha_0 = 1 + \sum_{i \in S_1} \omega_i$ and S_1 is the set of all $i \in \{1, 2, \dots, t\}$ such that $a_i = +1$. Similarly write $\beta = 2\beta_0 - \kappa$, $\gamma = 2\gamma_0 - \kappa$, $\delta = 2\delta_0 - \kappa$. We have

$$\begin{aligned} \alpha^2 &= 4\alpha_0^2 - 4\alpha_0\kappa + \kappa^2 = 4\alpha_0^2 + (n-4-8|S_1|)\kappa \\ &= 4 + 8|S_1| + 8 \sum_{i \in S_1} \omega_i + 4 \sum_{i \in S_1} \omega_{2i} + 4 \sum_{\substack{i, j \in S_1 \\ i > j}} (\omega_{i+j} + \omega_{i-j}) + (n-4-8|S_1|)\kappa \end{aligned}$$

and similarly for β, γ, δ using subsets $S_2, S_3, S_4 \subseteq \{1, 2, \dots, t\}$. By (ii), we have

$$\begin{aligned} 4n &= \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \\ &= 16 + 4(n-4)\kappa + 4 \sum_{k=1}^4 \left[(2-2\kappa)|S_k| + 2 \sum_{i \in S_k} \omega_i + \sum_{i \in S_k} \omega_{2i} + 2 \sum_{\substack{i, j \in S_k \\ i > j}} (\omega_{i+j} + \omega_{i-j}) \right]. \end{aligned}$$

Note that the constant term (i.e. the g^0 term) on the right side is $16 + 4(n-4) = 4n$, in agreement with the left side. Comparing coefficients of g^ℓ on both sides for $1 \leq \ell < n$ gives

$$0 = 4(n-4) - 8 \sum_{k=1}^4 |S_k| + 8s_\ell + 4s_{2\ell} + 8 \sum_{k=1}^4 |\{(i, j) \in S_k^2 : i > j, |i-\ell|=j\}|$$

where $s_\ell = 2 + \frac{1}{2}(a_\ell + b_\ell + c_\ell + d_\ell)$ is the number of k such that $\ell \in S_k$. Reading the last equation modulo 8, and recalling that n is odd, we deduce that s_ℓ is odd; that is, exactly three of the terms $a_\ell, b_\ell, c_\ell, d_\ell$ have the same sign, and the other has the opposite sign. Equivalently (see Exercise #3), the vector

$$(\tilde{a}_\ell, \tilde{b}_\ell, \tilde{c}_\ell, \tilde{d}_\ell) = (a_\ell, b_\ell, c_\ell, d_\ell)U, \quad U = \frac{1}{2} \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

has three zero coordinates and one coordinate ± 2 . Setting $(\tau_1, \tau_2, \tau_3, \tau_4) = (\alpha, \beta, \gamma, \delta)U$, we obtain four elements

$$\tau_1 = 1 + \sum_{\ell=1}^t \tilde{a}_\ell \omega_\ell, \quad \tau_2 = 1 + \sum_{\ell=1}^t \tilde{b}_\ell \omega_\ell, \quad \tau_3 = 1 + \sum_{\ell=1}^t \tilde{c}_\ell \omega_\ell, \quad \tau_4 = 1 + \sum_{\ell=1}^t \tilde{d}_\ell \omega_\ell$$

in $\mathbb{Z}[G]$ having exactly the form described by (iii). The converse (iii) \Rightarrow (ii) follows by reversing the steps. \square

Theorem 9.6 provides the following algorithm, demonstrated in the next two examples, to construct Hadamard matrices of order $4n \equiv 4 \pmod{8}$. Applying the trivial character $\chi : \mathbb{Z}[G] \rightarrow \mathbb{Z}$, $\sum_g a_g g \mapsto \sum_g a_g$ to the relation $\tau_1^2 + \tau_2^2 + \tau_3^2 + \tau_4^2 = 4n$ gives a representation of $4n$ as a sum of four odd squares $\sum_{k=1}^4 n_k^2$ where $n_k = \chi(\tau_k) \equiv 1 \pmod{4}$ is the trivial character value of τ_k (the sum of the integer coefficients of τ_k). We first therefore enumerate all representations of $4n$ as a sum of four odd squares. Next, we find $\tau_k \in \mathbb{Z}[G]$ of the form $1 \pm 2\omega_i \pm 2\omega_j \pm \dots$ with distinct subscripts, whose sums of coefficients give the required representations of $4n$ as a sum of four squares.

Example 9.7: A Hadamard matrix of Williamson type of order 20. Let $G = \langle g \rangle$ be cyclic of order $n = 5$. The unique representation of 20 as a sum of four odd squares (unique, that is, up to permutation of the four terms) is $20 = 1^2 + 1^2 + (-3)^2 + (-3)^2$. This gives a unique solution (again, up to permutation) of the relations (iii) in Theorem 9.6, namely $\tau_1 = \tau_2 = 1$, $\tau_3 = 1 - 2\omega_1$, $\tau_4 = 1 - 2\omega_2$ where $\omega_1 = g + g^4$ and $\omega_2 = g^2 + g^3$. We check that this unique feasible choice does indeed satisfy (iii):

$$\begin{aligned} \tau_1^2 + \tau_2^2 + \tau_3^2 + \tau_4^2 &= 1 + 1 + (1 - 2\omega_1)^2 + (1 - 2\omega_2)^2 = 4 - 4\omega_1 - 4\omega_2 + 4\omega_1^2 + 4\omega_2^2 \\ &= 4 - 4\omega_1 - 4\omega_2 + 4(\omega_2 + 2) + 4(\omega_1 + 2) = 20. \end{aligned}$$

We obtain

$$(\alpha, \beta, \gamma, \delta) = (\tau_1, \tau_2, \tau_3, \tau_4)U = (1 - \omega_1 - \omega_2, 1 - \omega_1 - \omega_2, 1 + \omega_1 - \omega_2, 1 - \omega_1 + \omega_2)$$

which yields

$$A = B = \begin{bmatrix} + & - & - & - & + \\ + & - & - & - & + \\ - & - & + & - & - \\ - & - & + & - & - \\ - & - & - & + & + \end{bmatrix}, \quad C = \begin{bmatrix} + & + & - & - & + \\ + & + & - & - & + \\ - & - & + & - & - \\ - & - & + & - & - \\ + & - & - & + & + \end{bmatrix}, \quad D = \begin{bmatrix} + & - & + & + & - \\ + & - & + & + & - \\ + & - & + & + & - \\ + & - & + & + & - \\ - & + & - & - & + \end{bmatrix}$$

and thereby a Hadamard matrix of Williamson type of order 20.

The same general strategy is used in the next example; except that with $n = 9$ in the following example, n is not prime (compare with $n = 5$ in the previous example) so a little more work is required. The required condition $\sum_{k=1}^4 \tau_k^2 = 4n$ in $\mathbb{Z}[G]$ is equivalent to $\sum_{k=1}^4 \chi(\tau_k)^2 = 4n$ as $\chi \in \widehat{G}$ ranges over a set of representatives of characters of orders dividing n (see Corollary 7.3). Thus in Example 9.8 we consider characters of order 1, 3 and then 9, in that order, refining our choices of the τ_k 's with each step. While these examples are intended to provide a taste of how this strategy might work in general, the reader should keep in mind that for all but the smallest values of n , this strategy is typically implemented by computer.

Example 9.8: Hadamard Matrices of order 36 of Williamson Type. Let $G = \langle g \rangle$ be cyclic of order $n = 9$. This group has an automorphism mapping $g \mapsto g^2$ which cycles $\omega_1 \mapsto \omega_2 \mapsto \omega_4 \mapsto \omega_1$ while fixing $\omega_3 \mapsto \omega_3$, thereby reducing the list of equivalence classes of the resulting Hadamard matrices. Representations of 36 as a sum of four odd squares include $(-3)^2 + (-3)^2 + (-3)^2 + (-3)^2$ and $1^2 + 1^2 + (-3)^2 + 5^2$, both of which lead to solutions of (iii). Here we consider only solutions of the second type such that $(\tau_1, \tau_2, \tau_3, \tau_4)$ has the form $(1, 1 - 2\omega_i + 2\omega_j, 1 - 2\omega_k, 1 + 2\omega_\ell)$ where $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$; and Exercise #4 covers the remaining cases not treated here. We require that

- (*) $1^2 + (1 - 2\omega_i + 2\omega_j)^2 + (1 - 2\omega_k)^2 + (1 + 2\omega_\ell)^2 = 36$; or equivalently,
- (**) $\chi(1)^2 + \chi(1 - 2\omega_i + 2\omega_j)^2 + \chi(1 - 2\omega_k)^2 + \chi(1 + 2\omega_\ell)^2 = 36$ for all $\chi \in \widehat{G}$.

The pattern chosen for the τ_k 's ensures that the trivial character satisfies (**) a fortiori; and before dealing with all 24 choices of indices in (*), we find that most of these cases can be eliminated readily using (**). Take now the character χ of order 3 with $\chi(g) = \zeta = \zeta_3$, so that $\chi(\omega_i) = \zeta + \zeta^2 = -1$ for $i = 1, 2, 4$; $\chi(\omega_3) = 2$. Thus

$$\begin{aligned} \text{(a)} \quad & \chi(1-2\omega_k)^2 = 9 \text{ for } k = 1, 2, 3, 4; \\ \text{(b)} \quad & \chi(1+2\omega_\ell)^2 = \begin{cases} 1, & \text{for } \ell = 1, 2, 4; \\ 25, & \text{for } \ell = 3; \end{cases} \\ \text{(c)} \quad & \chi(1-2\omega_i+2\omega_j)^2 = \begin{cases} 49, & \text{for } i \neq j = 3; \\ 25, & \text{for } i = 3 \neq j; \\ 1, & \text{for } i, j, 3 \text{ distinct.} \end{cases} \end{aligned}$$

We clearly require either $i = 3$ or $\ell = 3$. If $i = 3$ then $(i, j, k, \ell) = (3, 1, 2, 4)$ or $(3, 1, 4, 2)$ (or four other possibilities equivalent to these using the 3-cycle mentioned at the outset); but none of these cases satisfy (*). Indeed we may directly compute

$$\begin{aligned} & 1 + (1-2\omega_3+2\omega_1)^2 + (1-2\omega_2)^2 + (1+2\omega_4)^2 \\ &= 1 + (1+4\omega_3^2+4\omega_1^2-4\omega_3+4\omega_1-8\omega_3\omega_1) + (1-4\omega_2+4\omega_2^2) + (1+4\omega_4+4\omega_4^2) \\ &= 1 + 1 + 4(\omega_3+2) + 4(\omega_2+2) - 4\omega_3+4\omega_1-8(\omega_4+\omega_2) \\ &\quad + 1 - 4\omega_2 + 4(\omega_4+2) + 1 + 4\omega_4 + 4(\omega_4+2) \\ &= 36+8\omega_1-8\omega_2 \neq 0 \end{aligned}$$

and similarly for $(i, j, k, \ell) = (3, 1, 4, 2)$. If $\ell = 3$ then up to equivalence we have $(i, j, k, \ell) = (1, 2, 4, 3)$ or $(2, 1, 4, 3)$. More direct computation rules out the first of these cases; but the choice $(i, j, k, \ell) = (2, 1, 4, 3)$ is found to satisfy (*). So $(\tau_1, \tau_2, \tau_3, \tau_4) = (1, 1-2\omega_2+2\omega_1, 1-2\omega_4, 1+2\omega_3)$ gives a Hadamard matrix of order 36 of Williamson type.

Theorem 9.9 ([Wh]). For every prime power $q \equiv 1 \pmod{4}$ there exists a Hadamard matrix of order $4n = 2(q+1)$ of Williamson type.

Proof. Take $n = \frac{1}{2}(q+1)$ throughout, and note that n is odd. Consider the quadratic extension $E \supset F$ of fields of order q^2 and q respectively. Let $\chi : F \rightarrow \{0, \pm 1\}$ be the quadratic character. Choose a generator ω for the multiplicative group E^\times , so that $\omega_1 = \omega^{q+1}$ is a generator of F^\times . We abbreviate $\text{Tr} = \text{Tr}_{E/F} : x \mapsto x^q + x$ throughout. We define the sequence $u_k = \chi(\text{Tr} \omega^k)$ for $k \in \mathbb{Z}$. Recall that the quadratic character χ satisfies $\chi(\omega_1^k) = (-1)^k$ and so $u_{k+2n} = \chi(\text{Tr} \omega^{k+2n}) = \chi(\text{Tr}(\omega_1 \omega^k)) = \chi(\omega_1) \chi(\text{Tr} \omega^k) = \chi(\omega_1) \chi(\text{Tr} \omega^k) = -u_k$. Thus

$$(9.10) \quad u_{k+2n} = -u_k \text{ for all } k. \text{ In particular, the value of } u_k \text{ depends only on } k \pmod{4n}.$$

Since $\text{Tr} \omega^k = \omega^{qk} + \omega^k = \omega^{(q+1)k}(\omega^{-k} + \omega^{-qk}) = \omega_1^k \text{Tr} \omega^{-k}$, applying χ yields

$$(9.11) \quad u_{-k} = (-1)^k u_k \text{ for all } k.$$

The element $\theta = \omega^n$ satisfies $\theta^2 = \omega^{2n} = \omega_1$ and $\theta^q = \omega^{nq} = \omega^{(q^2-1)/2} \omega^n = -\theta$ so $\text{Tr} \theta = 0$. Now $\{1, \theta\}$ is a basis for E over F ; and $\text{Tr}(a + b\theta) = 2a$ for all $a, b \in F$. Note that for $z \in E$, we have $\chi(\text{Tr} z) = 0$ iff $\text{Tr} z = 0$ iff $z \in F\theta = \{b\theta : b \in F\}$. Thus

$$(9.12) \quad u_k = 0 \text{ for } k \equiv n \pmod{2n}; \text{ and otherwise, } u_k = \pm 1.$$

Next we want to evaluate

$$(9.13) \quad \sum_{z \in E} \chi(\text{Tr } z) \chi(\text{Tr}(\omega^r z)) \text{ for } z \in E, r \in \mathbb{Z}.$$

Writing $z = a + b\theta$, $\omega^r = c + d\theta$ with $a, b, c, d \in F$, the sum (9.13) takes the form

$$\begin{aligned} \sum_{a, b \in F} \chi(2a) \chi(2(ac + bd\omega_1)) &= \sum_{\substack{a, b \in F \\ a \neq 0}} \chi\left(\frac{1}{2a}\right) \chi(2(ac + bd\omega_1)) = \sum_{\substack{a, b \in F \\ a \neq 0}} \chi\left(c + \frac{bd\omega_1}{a}\right) \\ &= \begin{cases} q(q-1)\chi(c), & \text{if } d = 0; \\ 0, & \text{if } d \neq 0. \end{cases} \end{aligned}$$

Using the periodicity relation (9.10) and the fact that (9.13) vanishes at $z = 0$, the sum (9.13) simplifies to

$$2(q-1) \sum_{k=0}^{n-1} \chi(\text{Tr } \omega^k) \chi(\text{Tr}(\omega^{k+r})) = \begin{cases} q(q-1)\chi(c), & \text{if } d = 0; \\ 0, & \text{if } d \neq 0. \end{cases}$$

Also $\omega^r = c + d\theta \in F$ iff $r \equiv 0 \pmod{2n}$, in which case $\chi(2c) = \chi(\text{Tr } \omega^r) = (-1)^{r/2n}$; so

$$(9.14) \quad \sum_{k=0}^{n-1} u_k u_{k+r} = \begin{cases} (-1)^{\frac{r}{2n}} \chi(2)q, & \text{if } r \equiv 0 \pmod{2n}; \\ 0, & \text{otherwise.} \end{cases}$$

Now construct the four $n \times n$ matrices $A = \sum_{k=0}^{n-1} a_k T^k, \dots, D = \sum_{k=0}^{n-1} d_k T^k$ where

$$a_k = \begin{cases} 1, & \text{if } k \equiv 0 \pmod{n}; \\ u_{4k+n}, & \text{otherwise;} \end{cases} \quad b_k = \begin{cases} 1, & \text{if } k \equiv 0 \pmod{n}; \\ -u_{4k+n}, & \text{otherwise;} \end{cases} \quad c_k = d_k = u_{4k}, \text{ for all } k.$$

Note by (9.12) that all the values $a_k, b_k, c_k, d_k \in \{\pm 1\}$. Now

$$A^2 + B^2 + C^2 + D^2 = \sum_{r=0}^{n-1} \left(\sum_{k=0}^{n-1} (a_k a_{k+r} + b_k b_{k+r} + c_k c_{k+r} + d_k d_{k+r}) \right) T^r.$$

All the diagonal entries (for $r = 0$) are clearly $4n$; and for $r \neq 0$ we have

$$\sum_{k=0}^{n-1} (c_k c_{k+r} + d_k d_{k+r}) = 2 \sum_{k=0}^{n-1} u_{4k} u_{4k+4r} = 2 \sum_{\ell=0}^{n-1} u_\ell u_{\ell+r} = 0$$

using the permutation $k \mapsto \ell = 4k$ on $\mathbb{Z}/n\mathbb{Z}$. The remaining terms are

$$\begin{aligned} \sum_{k=0}^{n-1} (a_k a_{k+r} + b_k b_{k+r}) &= \sum_{\substack{0 < k < n \\ k \not\equiv -r \pmod{n}}} (a_k a_{k+r} + b_k b_{k+r}) \quad \text{since } a_r + b_r = u_{4r+n} - u_{4r+n} = 0 \\ &\quad \text{and } a_{-r} + b_{-r} = u_{-4r+n} - u_{-4r+n} = 0 \\ &= 2 \sum_{0 \leq k < n} u_{4k+n} u_{4k+4r+n} \quad \text{since } u_n = 0 \text{ by (9.12)} \\ &= 2 \sum_{\ell=0}^{n-1} u_\ell u_{\ell+r} = 0, \end{aligned}$$

again using a permutation $k \mapsto \ell = 4k + n$ of the index set $\mathbb{Z}/n\mathbb{Z}$. Now A, B, C, D are commuting circulant matrices which satisfy $A^2 + B^2 + C^2 + D^2 = 4nI_n$ as required. \square

Example 9.15: A Hadamard Matrix of order 12. Here we demonstrate Theorem 9.9 for $q = 5$, $n = \frac{1}{2}(q+1) = 3$. Take $\mathbb{F}_{25} = \mathbb{F}_5[\omega]$ where the primitive element ω satisfies $\omega^2 = \omega + 2$. The sequence u_0, u_1, u_2, \dots is $-+-0++++-+0---+0++++-+0-- --+- \dots$, giving $A=I-T-T^2$, $B=I+T+T^2$, $C=D=-I+T+T^2$. The construction of Theorem 9.9 gives

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} = \begin{bmatrix} +-- & +++ & -++ & +++ \\ --+ & +++ & +++ & +++ \\ --- & +-+ & +-- & +++ \\ --- & +-+ & +-+ & +++ \\ +++ & -++ & +-- & --- \\ ++ & +++ & + & --- \\ --- & +++ & --+ & --- \\ +-+ & +-+ & +++ & +-+ \\ +-+ & +-+ & +++ & +-+ \\ --- & --- & +++ & --- \end{bmatrix}.$$

Regular Hadamard Matrices

A Hadamard matrix is **regular** if all its row sums and all its column sums are equal. By Exercise #1, a regular Hadamard matrix is the same thing as a matrix of the form $H = A_+ - A_-$ where A_+ and A_- are incidence matrices of a complementary pair of symmetric $(4n^2, 2n^2 \pm n, n^2 \pm n)$ -designs. Each of these designs has order n .

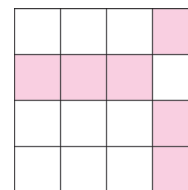
A regular Hadamard matrix may or may not arise from a difference set. When it does, it is given by a difference set with parameters $(4n^2, 2n^2 \pm n, n^2 \pm n)$ in a group of order $4n^2$. A difference set with these (very prolific) parameters is a **Menon difference set**, and the associated design a **Menon design**. (Warning: Many authors also refer to these as simply Hadamard difference sets, inviting confusion with the parameters $(4n-1, 2n-1, n-1)$ which also go by this name.) Up to complementation, it suffices to consider only the parameters $(4n^2, 2n^2 - n, n^2 - n)$. Note that interchanging $A_+ \leftrightarrow A_-$ switches $H \leftrightarrow -H$, but every Hadamard matrix is equivalent to its negative. Note also that in general, a regular Hadamard matrix may be equivalent to a Hadamard matrix which is not regular. Thus for example, (9.1) includes Hadamard matrices H_2 and H_4 of order 2 and 4 respectively; here H_4 is regular while the equivalent matrix $H_2 \otimes H_2$ is not.

The smallest regular Hadamard matrices of interest arises from symmetric $(16, 6, 2)$ -design, which in turn arises from a difference sets. Of the five equivalence classes of Hadamard matrices of order 16, three classes contain regular Hadamard matrices. One might argue that the one with the most symmetry is $H_4 \otimes H_4$ with $H_4 = J_4 - 2I_4$ as in the previous paragraph. We describe the symmetric design and difference sets giving rise to this example; and we comment only briefly on the other regular Hadamard matrices of order 16.

There are exactly three symmetric $(16, 6, 2)$ -designs, up to isomorphism. All of them arise from difference sets in multiple ways; these details may be found in [AK], [AS], [Ki].

Indeed, of the fourteen groups of order 16, all but two (the cyclic and dihedral groups) admit $(16, 6, 2)$ -difference sets in multiple ways. However, different groups and distinct difference sets in these groups can yield isomorphic designs. This is because a given design may admit more than one regular (i.e. sharply transitive) group of automorphisms; recall Theorem 8.5. What is true, however, is that the three nonisomorphic symmetric $(16, 6, 2)$ -designs yield three inequivalent regular Hadamard matrices. We describe just one of these, beginning with the design.

We construct a symmetric $(16, 6, 2)$ -design whose 16 points are the 16 cells of a 4×4 grid, as pictured on the right. The shaded cells in our picture indicate one of the sixteen blocks, where we have taken the symmetric difference of a row and a column. This can be done in 16 ways, generating thereby the 16 blocks: take the union of any row and any column, then



delete the single cell where they intersect. Verify mentally that every block contains 6 points; every point lies in 6 blocks; two distinct points have exactly 2 blocks in common; and two distinct blocks have exactly 2 points in common. There are twelve nonisomorphic groups that can act regularly on the points (and blocks) of this design, yielding twenty-four inequivalent difference sets. Here we consider only the possibilities with G abelian. Let $K_1 = \{1, a, b, c\}$ and $K_2 = \{1, a', b', c'\}$ be multiplicative groups of order 4 (any combination of cyclic groups and Klein 4-groups is fine) and let $G = K_1 \times K_2$. By choosing distinct symbols for the nonidentity elements in K_1 and K_2 , these subgroups can be identified with their images in $G = K_1 \times K_2$. Then $D = \{a, b, c, a', b', c'\}$ is a difference set in G with parameters $(16, 6, 2)$. If we denote $\kappa_1 = 1 + a + b + c \in \mathbb{Z}[K_1]$ and $\kappa_2 = 1 + a' + b' + c' \in \mathbb{Z}[K_2]$, then $\kappa := \kappa_1 \kappa_2 = \sum G$ and

$$\delta\delta^* = \delta^2 = (\kappa_1 + \kappa_2 - 2)^2 = 4\kappa_1 + 4\kappa_2 + 4 - 4\kappa_1 - 4\kappa_2 + 2\kappa_1\kappa_2 = 4 + 2\kappa,$$

verifying that D is a difference set in G with parameters $(16, 6, 2)$. If we let K_1 act regularly on the rows of the grid, and K_2 regularly on the columns, then $G = K_1 \times K_2$ acts regularly on the cells (i.e. points of the design) and D is the set of all $g \in G$ mapping P into B , for some choice of point P and block B . It is not hard to see that the resulting regular Hadamard matrix is $H_4 \otimes H_4$ in the notation of the previous paragraph.

Circulant Hadamard Matrices

A **circulant Hadamard matrix** is a circulant matrix that is also Hadamard. The only known examples have order 1 and 4, as in (9.1). It is clear that every circulant Hadamard matrix must be regular; and it must be constructed from a Menon difference set in a cyclic group of order $4n^2$ for some positive integer n . The **Circulant Hadamard Conjecture** poses that these do not exist for $n > 1$. Much work has been devoted to proving this conjecture; see [LeS], [S2]. (In related internet searches, beware of bogus proofs claiming to have already proved the conjecture.) In the smallest nontrivial case

$4n^2 = 16$, we noted above that there is no $(16, 6, 2)$ -difference set in a cyclic group of order 16. This result, long known, is attributed to Turyn.

Theorem 9.16. There is no cyclic difference set with parameters $(16, 6, 2)$, and hence no circulant Hadamard matrix of order 16.

Proof. Let $G = \{1, g, g^2, \dots, g^{15}\}$ be cyclic of order 16, and suppose there exists a difference set $D \subset G$ with parameters $(16, 6, 2)$. Then $\delta = \sum_{d \in D} d \in \mathbb{Z}[G]$ is a sum of six distinct elements in G satisfying $\delta\delta^* = 4 + 2\kappa$ where $\kappa = \sum_{i=0}^{15} g^i$. Let $\mathcal{O} = \mathbb{Z}[\zeta]$, $\zeta = \zeta_{16}$ and consider the character $\chi \in \widehat{G}$ of order 16 satisfying $\chi(g) = \zeta$. Denote $\alpha = \chi(\delta) = \sum_{d \in D} \chi(d) \in \mathcal{O}$. By Theorem 8.7, $|\alpha| = 2$. (Note here that $(v, k, r) = (16, 6, 2)$ and $n = 6 - 2 = 4$.) Much more than this, for every $\sigma \in \text{Aut } \mathbb{Q}[\zeta]$, we have $|\sigma(\alpha)| = 2$, since $\sigma \circ \chi : G \rightarrow \langle \zeta \rangle$ is also a nontrivial character of G .

Evaluating both sides of

$$\Phi_8(x) = x^8 + 1 = (x - \zeta)(x - \zeta^3)(x - \zeta^5) \cdots (x - \zeta^{15})$$

at 1 yields

$$2 = (1 - \zeta)(1 - \zeta^3)(1 - \zeta^5) \cdots (1 - \zeta^{15}).$$

By Theorem 4.3, all eight factors in the latter product are associates of $\varepsilon = 1 - \zeta$ in \mathcal{O} , yielding the factorization of principal ideals $(2) = (\varepsilon)^8$, so $N((\varepsilon)) = 2$ and the ideal $(\varepsilon) \subset \mathcal{O}$ is prime, the only distinct prime factor of (2) in \mathcal{O} (i.e. the prime 2 ramifies in $\mathbb{Q}[\zeta]$). Also $(\alpha)(\bar{\alpha}) = (4) = (\varepsilon)^{16}$, so comparing prime factors on both sides gives $(\alpha) = (\varepsilon)^r$ and $(\bar{\alpha}) = (\varepsilon)^s$ where $r + s = 16$. Now $2^r = N((\alpha)) = N((\bar{\alpha})) = 2^s$ so $r = s$ and $(\alpha) = (\bar{\alpha}) = (\varepsilon)^8 = (2)$. Since α and 2 are associates, $\alpha = 2u$ for some unit $u \in \mathcal{O}^\times$. Recalling that $|\sigma(\alpha)| = 2$ for all $\sigma \in \text{Aut } \mathbb{Q}[\zeta]$, we must have $|\sigma(u)| = 1$ for all $\sigma \in \text{Aut } \mathbb{Q}[\zeta]$. By Theorem 4.10, u is a root of unity in \mathcal{O} . By Theorem 4.2, $u = \zeta^k$ for some $k \in \{0, 1, 2, \dots, 15\}$. Without loss of generality, $\alpha = 2$; otherwise use Theorem 8.6 to replace D by $g^{-k}D$, another (equivalent) difference set in G with the same parameters $(16, 6, 2)$ satisfying $\chi(g^{-k}\delta) = \zeta^{-k}\alpha = 2$.

Now express δ in the form $\delta = \sum_{k=0}^{15} a_k g^k$ where $a_k \in \{0, 1\}$ with $\sum_{k=0}^{15} a_k = 6$, and note that $\zeta^8 = -1$ to get

$$(9.17) \quad 2 = \alpha = \chi(\delta) = \sum_{k=0}^{15} a_k \zeta^k = \sum_{k=0}^7 (a_k - a_{k+8}) \zeta^k.$$

Since the minimal polynomial of ζ over \mathbb{Q} is $x^8 + 1$, (9.17) requires $a_0 = 2 + a_8$ and $a_k = a_{k+8}$ for $k = 1, 2, \dots, 7$. Since $a_k \in \{0, 1\}$, this is impossible. \square

Although $\mathbb{Q}[\zeta_{16}]$ is known to be a UFD, we did not require this in the latter proof; all our factorizations were with regard to ideals.

Exercises 9.

1. Show that every Hadamard matrix of the form $H = I + S$ where $S^T = -S$ with first row $+++ \cdots +$ and first column $+- - \cdots -$ satisfies conditions (9.4) and (9.5). (Not much more needs to be said about (9.4), but (9.5) requires some explanation.)
2. Let H be a $v \times v$ regular Hadamard matrix, $v = 4N$. Suppose that H is regular; so by definition, there is an integer k such that every row and column of H has k ones and $v - k$ minus ones. Prove that the positions of the ones in H form the incidence matrix of a $(4n^2, 2n^2 \pm n, n^2 \pm n)$ -design; and the positions of the minus ones form the incidence matrix of the complementary $(4n^2, 2n^2 \mp n, n^2 \mp n)$ -design. In other words, show that $H = A_+ - A_-$ where $A_+ + A_- = J_v$ and the matrices A_+ and A_- are the incidence matrices of a pair of complementary $(4n^2, 2n^2 \pm n, n^2 \pm n)$ -designs.

Hint: Show that for any two distinct rows of H , the k minus ones in one row and the k minus ones in the other row overlap in exactly r positions where $r = k - N$. Show that the positions of the minus ones form the incidence matrix of a symmetric (v, k, r) design. Show that $N = (2N - k)^2$ using the feasibility relation of Section 8. Let $n = 2N - k$.

3. The **root lattice of type D_4** is the set L consisting of all vectors $\frac{1}{2}(a_1, a_2, a_3, a_4) \in \mathbb{R}^4$ such that a_1, a_2, a_3, a_4 are integers of the same parity (i.e. all even or all odd).
 - (a) Show that L is a 4-dimensional lattice; that is, there exists a basis $\{v_1, v_2, v_3, v_4\}$ of the real vector space \mathbb{R}^4 such that $L = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \mathbb{Z}v_3 + \mathbb{Z}v_4$.
 - (b) Show that for every $v \in L$, the squared Euclidean length $\|v\|^2$ is an integer.
 - (c) The **roots** of L are the vectors $v \in L$ of length 1. Show that there are sixteen roots, partitioned as $\Delta = \Delta_0 \sqcup \Delta_1$ where $|\Delta_0| = |\Delta_1| = 8$, $\Delta_0 \subset \mathbb{Z}^4$ and vectors in Δ_1 have half-integer coordinates.
 - (d) Consider the Hadamard matrix $H = J_4 - 2I_4$ of order 4 given at the start of this section. Show that the matrix $U = \frac{1}{2}H$ represents an isometry (i.e. distance-preserving transformation) on \mathbb{R}^4 , which preserves L ; in particular, U permutes the roots of L . Show moreover that U interchanges the two subsets $\Delta_0 \leftrightarrow \Delta_1$ of the roots.
4. Complete the enumeration of Hadamard matrices of order 36 of Williamson type begun in Example 9.8.
 - (a) Show that the representation $36 = (-3)^2 + (-3)^2 + (-3)^2 + (-3)^2$ leads to a unique solution $(\tau_1, \tau_2, \tau_3, \tau_4) = (1 - 2\omega_1, 1 - 2\omega_2, 1 - 2\omega_3, 1 - 2\omega_4)$ up to permutation of the four indices, leading to a Hadamard matrix of order 36 of Williamson type.
 - (b) Show that the representation $36 = 1^2 + 1^2 + (-3)^2 + 5^2$ leads to just one more possibility other than the one we considered in Example 9.8, namely $(1, 1, 1 - 2\omega_i, 1 - 2\omega_j + 2\omega_k + 2\omega_\ell)$. Does this case actually yield any Hadamard matrices? Explain.

10. Quadratic Reciprocity

Let $F = \mathbb{F}_p$ be the field of odd prime order p , i.e. the integers mod p . (Some of the results of this section will be extended to more general odd-order fields in Section 11.) We recall some properties of F from Section 3: The group of units F^\times is cyclic of order $p - 1$, partitioned as $F^\times = S \sqcup N$ where S and N consist of the nonzero squares and the nonzsquares respectively. We have $|S| = |N| = \frac{1}{2}(p - 1)$. Here $S < F^\times$ is the subgroup of index 2, with N the nontrivial coset of S . We have the quadratic character $\chi : F \rightarrow \mathbb{C}$ where $\chi(a) = 0, 1$ or -1 according as $a = 0, a \in S$ or $a \in N$.

If we compose χ with the canonical homomorphism of additive groups $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} = F$, we get the **Legendre symbol** defined for every integer a by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } a \equiv 0 \pmod{p}; \\ 1, & \text{if } a \text{ is a nonzero square mod } p; \\ -1, & \text{if } a \text{ is a nonsquare mod } p. \end{cases}$$

The fact that $\chi : \mathbb{Z} \rightarrow \mathbb{C}^\times$ is multiplicative is a simple consequence of the fact that it is a composite of two multiplicative maps. The lifting of χ (the quadratic character on the finite field F) to all of \mathbb{Z} , is an example of a Dirichlet character (see Appendix 6). In this context, squares and nonsquares (mod p) are traditionally called *quadratic residues* and *nonquadratic residues*; but unfortunately the latter is often abbreviated to *nonresidues*, which is strictly a misnomer. We will simply speak of nonzero squares and nonsquares mod p . The strict definition of the Legendre symbol usually excludes the case $a \equiv 0 \pmod{p}$; but a natural generalization of $\left(\frac{a}{p}\right)$ called the *Jacobi symbol* allows this case, and so do we. (But we will have nothing more to say about the Jacobi symbol in these notes.)

As with the quadratic character on F , several other properties of F underlie basic properties of the ring \mathbb{Z} . For example **Fermat's Little Theorem**, in the form

$$(10.1) \quad a^{p-1} \equiv 1 \pmod{p} \text{ for every integer } a \not\equiv 0 \pmod{p}, p \text{ prime,}$$

is a direct consequence of the fact that F^\times is a group of order $p-1$. And from (10.1) we immediately obtain the equivalent form of Fermat's Little Theorem,

$$(10.2) \quad a^p \equiv a \pmod{p} \text{ for every integer } a, \text{ where } p \text{ is any prime.}$$

Also the formula $\chi(a) = a^{(p-1)/2}$ in F , restated in the context of rational integers, gives **Euler's Criterion**:

$$(10.3) \quad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \text{ for every integer } a.$$

We restate the multiplicativity of the Legendre symbol, which follows either from facts about F or from (10.3):

$$(10.4) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \text{ for all integers } a, b.$$

The main result of this Section is

Theorem 10.5. Let p and q be distinct odd primes. Then

- (a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}; \\ -1, & \text{if } p \equiv 3 \pmod{4}; \end{cases}$
- (b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}; \end{cases}$
- (c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} 1, & \text{if at least one of } p, q \text{ is } \equiv 1 \pmod{4}; \\ -1, & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$

Part (c) is properly known as the **Law of Quadratic Reciprocity**; and we include (a) and (b) for completeness. There are currently hundreds of proofs of this result known—probably more proofs than any result other than the Theorem of Pythagoras. A current census lists 246 distinct proofs:

<http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html>

Gauss himself gave many different proofs; and the proof we give here is his sixth proof, although it has been rediscovered by many others since then. Before proving this result, we demonstrate its utility for computing specific values of the Legendre symbol:

Example 10.6: Computing the Legendre symbol using the Law of Quadratic Reciprocity.

Evaluate each of the values $(\frac{a}{331})$ for $a = 83, 101$ and 146 , noting that 331 is prime.

Solutions: $(\frac{83}{331}) = -(\frac{331}{83}) = -(\frac{82}{83}) = -(-\frac{1}{83}) = -(-1) = 1.$

$(\frac{101}{331}) = (\frac{331}{101}) = (\frac{28}{101}) = (\frac{2}{101})^2(\frac{7}{101}) = (\frac{101}{7}) = (\frac{3}{7}) = -(\frac{7}{3}) = -(\frac{1}{3}) = -1.$

$(\frac{146}{331}) = (\frac{2}{331})(\frac{73}{331}) = (-1)(\frac{331}{73}) = -(\frac{39}{73}) = -(\frac{3}{73})(\frac{13}{73}) = -(\frac{73}{3})(\frac{73}{13}) = -(\frac{1}{3})(\frac{8}{13}) = -(\frac{2}{13})^3 = -(-1)^3 = 1.$

The utility of the Law of Quadratic Reciprocity for computing values of the Legendre symbol is primarily for using hand computation with small examples such as these. For larger integers, Euler's Criterion (10.3) is much easier to implement by computer; and it avoids the difficulty of having to perform integer factorization on larger numbers (which is prohibitive for integers of hundreds of digits). But of course, the Law of Quadratic Reciprocity has many uses beyond such numerical examples as these.

Example 10.7: Factoring quadratic polynomials mod p . Factor each of the polynomials $x^2 + 13x + 17$ and $3x^2 + 13x + 16$ in $\mathbb{F}_{823}[x]$.

Solution: $x^2 + 13x + 17$ has discriminant $13^2 - 4 \cdot 17 = 101$ where

$$(\frac{101}{823}) = (\frac{823}{101}) = (\frac{15}{101})(\frac{5}{101}) = (\frac{101}{3})(\frac{101}{5}) = (\frac{2}{3})(\frac{1}{5}) = (-1)(1) = -1.$$

This polynomial has no roots in \mathbb{F}_{823} since its discriminant is a nonsquare; so it is irreducible in $\mathbb{F}_{823}[x]$.

The polynomial $3x^2 + 13x + 16$ has discriminant $13^2 - 4 \cdot 3 \cdot 16 = -23$ where

$$(\frac{-23}{823}) = (\frac{-1}{823})(\frac{23}{823}) = (-1) \left[-(\frac{823}{23}) \right] = (\frac{18}{23}) = (\frac{2}{23})(\frac{3}{23})^2 = (1)(-1)^2 = 1.$$

Since the discriminant is a nonzero square in \mathbb{F}_{823} , there are two distinct roots mod 823. Other computational methods (see Exercise #3) confirm that $\frac{1}{6}(-13 \pm \sqrt{-23}) = 533, 560$ are the two roots in \mathbb{F}_{823} , yielding the factorization $3x^2 + 13x + 16 = 3(x - 533)(x - 560) = 3(x + 290)(x + 263)$.

Our proof of Theorem 10.5 will require some preparation. First note that

$$(10.8) \quad \sum_{k=0}^{p-1} \binom{k}{p} = \binom{0}{p} + \binom{1}{p} + \binom{2}{p} + \cdots + \binom{p-1}{p} = 0$$

since the sum includes one 0 term, $\frac{p-1}{2}$ terms equal to $+1$, and $\frac{p-1}{2}$ terms equal to -1 . Next recall that if $a \not\equiv 0 \pmod{p}$, then ζ^a is a primitive p th root of unity, hence a root of $\Phi_p(x)$; so

$$(10.9) \quad 1 + \zeta^a + \zeta^{2a} + \cdots + \zeta^{(p-1)a} = 0.$$

Next, following Gauss, we consider the sum

$$(10.10) \quad S = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \zeta^k = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k;$$

thus for example $S = \zeta - \zeta^2 - \zeta^3 + \zeta^4$ when $p = 5$. Sums of the form (10.10) are called **quadratic Gauss sums**. Gauss himself proved

$$\textbf{Lemma 10.11.} \quad S^2 = \left(\frac{-1}{p}\right)p = \begin{cases} p, & \text{if } p \equiv 1 \pmod{4}; \\ -p, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. We expand

$$\begin{aligned} S^2 &= \left[\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k \right] \left[\sum_{\ell=0}^{p-1} \left(\frac{\ell}{p}\right) \zeta^\ell \right] \\ &= \sum_{k=1}^{p-1} \sum_{\ell=0}^{p-1} \left(\frac{k}{p}\right) \left(\frac{\ell}{p}\right) \zeta^{k+\ell} \\ &= \sum_{k=1}^{p-1} \sum_{\ell=0}^{p-1} \left(\frac{k\ell}{p}\right) \zeta^{k+\ell} \quad (\text{by (10.4)}) \\ &= \sum_{k=1}^{p-1} \sum_{m=0}^{p-1} \left(\frac{k^2 m}{p}\right) \zeta^{k+km} \quad (\text{substituting } \ell = km) \\ &= \sum_{k=1}^{p-1} \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^{(1+m)k} \\ &= \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \left[\sum_{k=1}^{p-1} \zeta^{(1+m)k} \right]. \end{aligned}$$

Now if $m \neq p-1$ then the inner sum $\sum_{k=1}^{p-1} \zeta^{(1+m)k} = -1$ by (10.9), whereas if $m = p-1$ we have $\sum_{k=1}^{p-1} \zeta^{(1+m)k} = \sum_{k=1}^{p-1} 1 = p-1$. This leaves

$$\begin{aligned} S^2 &= - \sum_{m=0}^{p-2} \left(\frac{m}{p}\right) + \left(\frac{p-1}{p}\right)(p-1) \\ &= \left(\frac{p-1}{p}\right) + \left(\frac{p-1}{p}\right)(p-1) \quad (\text{by (10.8)}) \\ &= \left(\frac{p-1}{p}\right)p. \end{aligned} \quad \square$$

By Lemma 10.11,

$$S = \begin{cases} \pm\sqrt{p}, & \text{if } p \equiv 1 \pmod{4}, \\ \pm i\sqrt{p}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

The ambiguous signs in this formula stare us in the face, begging to be resolved. This is a natural and compelling problem, which perplexed Gauss for years before finally the answer came to him. As Gauss wrote to a friend in 1805:

The determination of the sign of the root has vexed me for many years. This deficiency overshadowed everything that I found: over the last four years, there was rarely a week that I did not make one or another attempt, unsuccessfully, to untie the knot. I succeeded—but not as a result of my search but rather, I should say, through the mercy of God. As lightning strikes, the riddle has solved itself.

The conclusive result, as Gauss showed, has ‘+’ in place of each of the signs ‘±’ above; however for the purpose of proving the Law of Quadratic Reciprocity, the less definitive version stated in Lemma 10.11 above suffices.

Before proceeding further, here is our last preparatory result:

$$(10.12) \quad \text{For every prime } q, (x + y)^q \equiv x^q + y^q \pmod{q\mathbb{Z}[x, y]}.$$

This follows from the binomial expansion of $(x + y)^q$, using the fact that all binomial coefficients $\binom{q}{k} = \frac{q!}{k!(q-k)!}$ are divisible by q for $k \in \{1, 2, \dots, q-1\}$. This argument has appeared in the proof of Theorem 3.7, but here our setting is a little more general: our x and y are not in \mathbb{F}_{p^e} , nor are they in \mathbb{Z} ; they are indeterminates. So (10.12) is sufficiently general as to apply in an arbitrary commutative ring. We will in particular evaluate (10.12) for $x, y \in \mathbb{Z}[\zeta_p]$ in the course of the following proof.

Proof of Theorem 10.5. Let p, q be distinct odd primes, and consider the Gauss sum $S = \sum_{k=0}^{p-1} \binom{k}{p} \zeta^k \in \mathcal{O}$ as in (10.11), where $\mathcal{O} = \mathbb{Z}[\zeta]$, $\zeta = \zeta_p$. Taking the $\frac{q-1}{2}$ power of the relation in the Lemma 10.11 gives

$$S^{q-1} = (S^2)^{(q-1)/2} = \left(\frac{-1}{p}\right)^{(q-1)/2} p^{(q-1)/2} \equiv (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \pmod{q\mathcal{O}}.$$

Multiplying both sides by S gives

$$\begin{aligned} (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) S &\equiv S^q \\ &\equiv \sum_{k=0}^{q-1} \binom{k}{p}^q \zeta^{qk} \quad (\text{by (10.12)}) \\ &\equiv \sum_{k=0}^{q-1} \binom{k}{p} \zeta^{qk} \quad (\text{since } q \text{ is odd}) \\ &\equiv \sum_{k=0}^{q-1} \binom{kq^2}{p} \zeta^{qk} \quad (\text{since } q \not\equiv 0 \pmod{p}) \end{aligned}$$

$$\begin{aligned} &\equiv \sum_{\ell=0}^{q-1} \left(\frac{\ell q}{p}\right) \zeta^\ell \quad (\text{substituting } \ell = kq) \\ &\equiv \sum_{\ell=0}^{q-1} \left(\frac{\ell}{q}\right) \left(\frac{q}{p}\right) \zeta^\ell \quad (\text{by (10.4)}) \\ &\equiv \left(\frac{q}{p}\right) S \pmod{q\mathcal{O}}. \end{aligned}$$

Again we multiply both sides by S to obtain

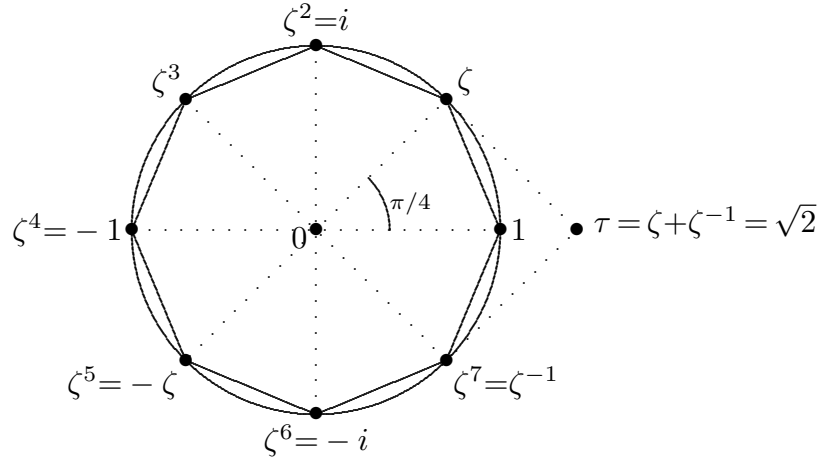
$$(-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) S^2 \equiv \left(\frac{q}{p}\right) S^2 \pmod{q\mathcal{O}}$$

and since $S^2 = \left(\frac{-1}{p}\right)p$, which is an integer relatively prime to q , this gives

$$(-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q\mathcal{O}}.$$

All factors on both sides of this expression are ± 1 so this gives part (c) of the Theorem.

Part (a) of the Theorem follows immediately from Euler's Criterion (10.3). For (b), let $\mathcal{O} = \mathbb{Z}[\zeta]$, $\zeta = \zeta_8 = e^{\pi i/4} = \frac{1+i}{\sqrt{2}}$; and let $\tau = \zeta + \zeta^{-1} = \sqrt{2}$.



By Euler's Criterion (10.3),

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv \tau^{p-1} \pmod{p\mathcal{O}}$$

so by (10.12),

$$\left(\frac{2}{p}\right) \tau \equiv \tau^p \equiv (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p\mathcal{O}}.$$

Since ζ is an eighth root of unity, we obtain

$$\left(\frac{2}{p}\right) \tau \equiv (-1)^{(p^2-1)/8} \tau \pmod{p\mathcal{O}}$$

where

$$(-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Multiplying both sides by τ gives $2\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8} 2 \pmod{p\mathcal{O}}$; and since 2 is relatively prime to p , (b) follows. \square

Throughout our proof, ‘mod $p\mathcal{O}$ ’ and ‘mod $q\mathcal{O}$ ’ can be read as ‘mod p ’ and ‘mod q ’ respectively. The careful reader will observe that for $x, y \in \mathbb{Z}$, we have $x \equiv y \pmod{p\mathcal{O}}$ iff $x \equiv y \pmod{p}$ in the usual sense; this is because $\mathbb{Z} \cap p\mathcal{O} = p\mathbb{Z}$.

We now resolve the sign of S . Until now we have required only that ζ is a root of $\Phi_p(t)$ in some extension of \mathbb{Q} (as this completely determines the algebraic structure of $\mathbb{Q}(\zeta) \supset \mathbb{Q}$). In order to resolve the ambiguous sign of $S = \sum_k \left(\frac{k}{p}\right) \zeta^k$, we must fix a choice of ζ . This choice needs to be made using extraneous (i.e. non-algebraic) properties of elements of our extension, such as ordering, as without such considerations, all choices of ζ (and choices of the sign of S) are equivalent under field automorphisms. The elusiveness of the proof of Theorem 10.13 may be attributed to the inaccessibility of this result from purely algebraic arguments within $\mathbb{Q}(\zeta)$.

Theorem 10.13. Fix $\zeta = e^{2\pi i/p}$ where p is an odd prime, and let $S = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k$. Then

$$S = \begin{cases} \sqrt{p}, & \text{if } p \equiv 3 \pmod{4}; \\ i\sqrt{p}, & \text{if } p \equiv 1 \pmod{4}. \end{cases}$$

We present the proof found in [IR, Section 6.4]. Other proofs are available; for example Dirichlet gave a proof using Fourier analysis. The proof in [LN, Theorem 5.15] uses some representation theory. The correct generalization of Theorem 10.13 to all fields of odd order is proved in Section 12 using the Hasse-Davenport relations.

Proof of Theorem 10.13. Evaluate $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1} = \prod_{r=1}^{p-1} (x - \zeta^r)$ at 1 to get

$$\begin{aligned} p = \Phi_p(1) &= \prod_{r=1}^{p-1} (1 - \zeta^r) = \prod_{j=1}^{p-1} (1 - \zeta^{4j}) = \prod_{j=1}^{\frac{p-1}{2}} (1 - \zeta^{4j}) \prod_{k=\frac{p+1}{2}}^{p-1} (1 - \zeta^{4k}) \\ &= \prod_{\ell=1}^{\frac{p-1}{2}} (1 - \zeta^{2p+2-4\ell}) \prod_{m=1}^{\frac{p-1}{2}} (1 - \zeta^{2p-2+4m}) \quad \left(\begin{array}{l} \text{substitute } \ell = \frac{p+1}{2} - j \\ \text{and } k = \frac{p-1}{2} + m \end{array} \right) \\ &= \prod_{k=1}^{\frac{p-1}{2}} (1 - \zeta^{2-4k})(1 - \zeta^{4k-2}) = \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{1-2k})(\zeta^{1-2k} - \zeta^{2k-1}) \\ &= (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{1-2k})^2. \end{aligned}$$

This says that

$$(2i)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} \sin\left(\frac{4k-2}{p}\pi\right) = \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{1-2k}) = \pm i^{\frac{p-1}{2}} \sqrt{p}$$

where the factor $\sin(\frac{4k-2}{p}\pi)$ is negative iff $\frac{p+3}{4} \leq k \leq \frac{p-1}{2}$; and the number of integers k in this range is $\lfloor \frac{p-3}{4} \rfloor$. Thus

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{1-2k}) = (-1)^{\lfloor \frac{p-3}{4} \rfloor} i^{\frac{p-1}{2}} \sqrt{p} = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod{4}; \\ i\sqrt{p}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

This is exactly the conjectured value of S ; and combining this with Lemma 10.11 and the remarks following it,

$$S = \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{1-2k})$$

where $\varepsilon = \pm 1$. Our task is to prove that $\varepsilon = 1$. Following Kronecker, we introduce the polynomial

$$f(x) = \sum_{j=1}^{p-1} \binom{j}{p} x^j - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (x^{2k-1} - x^{p-2k+1}).$$

Note that $f(1) = 0$ by (10.8), and $f(\zeta) = 0$ by definition of ε ; so $f(x)$ is divisible by $(x-1)\Phi_p(x) = x^p - 1$. Write $f(x) = (x^p - 1)h(x)$ where $h(x) \in \mathbb{Q}[x]$. In fact $h(z) \in \mathbb{Z}[x]$ by Lemma A2.1(iii). Evaluating at $x = e^z$,

$$(10.14) \quad \sum_{j=1}^{p-1} \binom{j}{p} e^{jz} - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (e^{(2k-1)z} - e^{(p-2k+1)z}) = (e^{pz} - 1)h(e^z).$$

Using power series expansions, compare the coefficient of $z^{\frac{p-1}{2}}$ on both sides of (10.14). On the right side, we first write $h(x) = \sum_{j=0}^m b_j x^j$ where $b_0, b_1, \dots, b_m \in \mathbb{Z}$; then

$$h(e^z) = \sum_{j=0}^m b_j e^{jz} = \sum_{j=0}^m \sum_{k=0}^{\infty} b_j \frac{(jz)^k}{k!} = \sum_{k=0}^{\infty} c_k \frac{z^k}{k!}, \quad c_k = \sum_{j=0}^m b_j j^k \in \mathbb{Z}$$

and so

$$(e^{pz} - 1)h(e^z) = \sum_{j=1}^{\infty} \frac{p^j z^j}{j!} \sum_{k=0}^{\infty} c_k \frac{z^k}{k!} = \sum_{\ell=1}^{\infty} d_{\ell} \frac{z^{\ell}}{\ell!}, \quad d_{\ell} = \sum_{j=1}^{\ell} p^j c_{\ell-j} \in \mathbb{Z}.$$

Clearly each $d_{\ell} \equiv 0 \pmod{p}$. Equating coefficients of $z^{\frac{p-1}{2}}$ on both sides of (10.14), and then multiplying both sides by $\frac{p-1}{2}!$, we find

$$\underbrace{\sum_{j=0}^{p-1} \binom{j}{p} j^{\frac{p-1}{2}}}_{(10.15)} - \underbrace{\frac{p-1}{2}! \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (4k-p-2)}_{(10.16)} = d_{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

since $e^{(2k-1)z} - e^{(p-2k+1)z} = (4k-p+2)z + O(z^2)$. Now (10.15) simplifies as

$$\sum_{j=0}^{p-1} \binom{j}{p} j^{\frac{p-1}{2}} \equiv \sum_{j=0}^{p-1} \binom{j}{p} \binom{j}{p} \equiv \sum_{j=0}^{p-1} 1 = -1 \pmod{p}$$

by Euler's Criterion, while (10.16) reduces as

$$\begin{aligned} \frac{p-1}{2}! \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (4k-p-2) &\equiv \frac{p-1}{2}! \varepsilon \cdot 2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} (2k-1) = \frac{p-1}{2}! \varepsilon \cdot 2^{\frac{p-1}{2}} \frac{(p-1)!}{2 \cdot 4 \cdot 6 \cdots (p-1)} \\ &= (p-1)! \varepsilon \equiv -\varepsilon \pmod{p} \end{aligned}$$

using Wilson's Theorem (Exercise #3.1(b)). So our original congruence relating (10.15) and (10.16) simplifies as $-1 + \varepsilon \equiv 0 \pmod{p}$. Since $\varepsilon = \pm 1$ and p is an odd prime, this forces $\varepsilon = 1$, which completes our proof. \square

Exercises 10.

- Evaluate each of the following Legendre symbols *by hand* as done in Example 10.6. Then use appropriate computer software with arbitrary precision arithmetic capability to *check* your answer by Euler's Criterion (10.3).
 - $\left(\frac{59}{89}\right)$
 - $\left(\frac{-7}{233}\right)$
 - $\left(\frac{111}{347}\right)$
 - $\left(\frac{620}{503}\right)$
 - $\left(\frac{709}{809}\right)$
- Using the Law of Quadratic Reciprocity, show that a prime p admits solutions of the congruence $x^2 \pm x + 1 \equiv 0 \pmod{p}$ iff $p = 3$ or $p \equiv 1 \pmod{3}$.
 - Now consider a finite field $F = \mathbb{F}_q$ where $q = p^e$, and assume that $p \neq 3$. Show that solutions of $x^2 + x + 1 = 0$ in F are primitive cube roots of unity in F ; and solutions of $x^2 - x + 1 = 0$ are primitive sixth roots of unity in F .
 - Using the fact that the multiplicative group F^\times is cyclic, show that F has a primitive cube root of unity iff $q \equiv 1 \pmod{3}$; and F has a primitive sixth root of unity iff $q \equiv 1 \pmod{6}$. (This requires only elementary properties of cyclic groups.) Conclude that a finite field F of order q has solutions of $x^2 \pm x + 1 = 0$ iff $q \equiv 1 \pmod{3}$.
- Complete the remaining steps of Example 10.7, *using appropriate computer software with arbitrary precision arithmetic capability*.
 - According to Example 10.7, $\left(\frac{-23}{823}\right) = 1$. Confirm this fact using Euler's Criterion (10.3), by computing $(-23)^{411} \pmod{823}$. (Note: $411 = \frac{1}{2}(823 - 1)$.)
 - Using (a), evaluate $(-23)^{412} \pmod{823}$, noting that $412 = 411 + 1$.
 - Now evaluate $(-23)^{206} \pmod{823}$, noting that $206 = 412/2$.
 - Using the previous steps, find the two square roots of $-23 \pmod{823}$.
 - Find the two roots of $3x^2 + 13x + 16 \in \mathbb{F}_{823}[x]$.
 - Generalizing your work, present to an algorithm for computing square roots mod p for an arbitrary prime $p \equiv 3 \pmod{4}$. Explain why this algorithm works.

11. Gauss and Jacobi Sums

Each finite field $E = \mathbb{F}_q$ gives rise to two finite groups, the additive group E of order q and the multiplicative group E^\times of order $q - 1$. Characters of these groups are called **additive characters** and **multiplicative characters** respectively. Much of the interplay between these two groups is encoded in the language of Gauss sums. Following the notation of

Section 6, the additive characters form a multiplicative group \widehat{E} , elementary abelian of order q , whose elements $\psi \in \widehat{E}$ satisfy

$$\psi(x + y) = \psi(x)\psi(y)$$

for all $x, y \in E$. Multiplicative characters form a cyclic multiplicative group \widehat{E}^\times of order $q - 1$ whose elements $\chi \in \widehat{E}^\times$ satisfy

$$\chi(xy) = \chi(x)\chi(y)$$

for all $x, y \in E^\times$. The latter formula holds for all $x, y \in E$ if we naturally extend the domain of multiplicative characters by the convention that

$$\chi(0) = \begin{cases} 1, & \text{if } \chi = \chi_0, \text{ the identity element of } \widehat{E}^\times; \\ 0, & \text{otherwise.} \end{cases}$$

Note that the trivial multiplicative character $\chi_0 \in \widehat{E}^\times$ satisfies $\chi_0(x) = 1$ for all $x \in E$.

In the following, we fix the prime field $F = \mathbb{F}_p$ where $q = p^e$; and abbreviate $\text{Tr} = \text{Tr}_{E/F} : E \rightarrow F$ throughout, as in Theorem A1.7. By Theorem 3.8, the absolute trace map satisfies $\text{Tr}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{e-1}}$. Also recall that by Theorem 3.2, the field has a cyclic multiplicative group $E^\times = \langle \omega \rangle$.

Lemma 11.1. (i) The q additive characters of E have the form $\psi_a(x) = \zeta_p^{\text{Tr}(ax)}$ for $a \in E$.

(ii) Fix a generator ω for E^\times . Then the $q - 1$ multiplicative characters of E have the form $\chi_k(\omega^r) = \zeta_{q-1}^{kr}$ for $k \in \mathbb{Z}/(q-1)\mathbb{Z}$; and $\chi_k(0) = 0$ for $1 \leq k < q - 1$.

In particular, additive characters have values in $\mathbb{Z}[\zeta_p]$; and multiplicative characters have values in $\mathbb{Z}[\zeta_{q-1}]$. More precisely, if $d = \gcd(k, q-1)$, then χ_k has values in $\mathbb{Z}[\zeta_{(q-1)/d}]$.

We refer to χ_k ($k \neq 0$) as a **character of order** $\frac{q-1}{d} = \frac{\text{lcm}(k, q-1)}{k}$ where $d = \gcd(k, q-1)$, since $\frac{q-1}{d}$ is the order of χ_k in the group \widehat{E}^\times . In this notation, χ_{q-1} is another name for the trivial multiplicative character χ_0 described above. For q odd, $\chi_{\frac{q-1}{2}}$ is the quadratic character. The trivial additive character is $\psi_0(x) = 1$.

Proof of Lemma 11.1. Clearly each $\psi_a \in \widehat{E}$, and the trivial additive character is $\psi_0(x) = 1$ for all $x \in E$. If $a \neq b$ in E then by Theorem A1.7(ii), there exists $x \in E$ satisfying $\text{Tr}[(a-b)x] \neq 0$, so $\frac{\psi_a(x)}{\psi_b(x)} = \psi_{a-b}(x) \neq 1$ and $\psi_a \neq \psi_b$. So the additive characters $\psi_a \in \widehat{E}$ ($a \in E$) are distinct; and since $|\widehat{E}| = q$ by Theorem 6.1(b), all additive characters have this form. This proves (i), and (ii) is similar. \square

For $\chi \in \widehat{E}^\times$ and $\psi \in \widehat{E}$, we define the **Gauss sums**

$$G(\chi, \psi) = \sum_{x \in E} \chi(x)\psi(x) \in \mathbb{Z}[\zeta_p, \zeta_{q-1}] = \mathbb{Z}[\zeta_{(q-1)p}]; \quad G(\chi) = G(\chi, \psi_1) = \sum_{x \in E} \chi(x)\zeta^{\text{Tr } x}.$$

This generalizes the quadratic Gauss sum S from Section 10. Questions about $G(\chi, \psi)$ can usually be reduced to questions about $G(\chi)$, due to (i) below.

Theorem 11.2. (i) If $\chi \neq \chi_0$ or $a \neq 0$, then $G(\chi, \psi_a) = \bar{\chi}(a)G(\chi) = \overline{\chi(a)}G(\chi)$.
(ii) $\overline{G(\chi)} = \chi(-1)G(\bar{\chi})$.

Proof. (i) If $a \neq 0$ then $G(\chi, \psi_a) = \sum_{x \in E} \chi(x) \zeta^{\text{Tr}(ax)} = \sum_{u \in E} \chi\left(\frac{u}{a}\right) \zeta^{\text{Tr} u} = \frac{1}{\chi(a)} G(\chi) = \overline{\chi(a)} G(\chi)$. Now suppose $a = 0$, so $G(\chi, \psi_0) = \sum_{x \in E} \chi(x)$. If $\chi \neq \chi_0$ then by the convention above, $\chi(0) = 0$ and the remaining terms cancel since χ and χ_0 are orthogonal by Theorem 6.2(a), so again the conclusion holds.

(ii) $\overline{G(\chi)} = \sum_{x \in E} \overline{\chi(x) \zeta^{\text{Tr} x}} = \sum_{x \in E} \bar{\chi}(x) \zeta^{-\text{Tr} x} = G(\bar{\chi}, \psi_{-1}) = \overline{\chi(-1)} G(\bar{\chi}) = \chi(-1) G(\bar{\chi})$ using (i) and the fact that $\chi(-1) = \pm 1$. \square

Theorem 11.3. Let $\chi \in \widehat{E^\times}$, $\psi \in \widehat{E}$, and assume $\chi \neq \chi_0$, $\psi \neq \psi_0$. Then

- (i) $|G(\chi, \psi)| = \sqrt{q}$.
- (ii) $G(\chi, \psi_0) = 0$.
- (iii) $G(\chi_0, \psi) = 0$.
- (iv) $G(\chi_0, \psi_0) = q$.

Proof. (ii) $G(\chi, \psi_0) = \sum_{x \in E^\times} \chi(x) = 0$ since χ and χ_0 are orthogonal (Theorem 6.2(a)).

(iii) $G(\chi_0, \psi) = \sum_{x \in E} \psi(x) = 0$ since ψ and ψ_0 are orthogonal (Theorem 6.2(a)).

(iv) $G(\chi_0, \psi_0) = \sum_{x \in E} 1 = q$.

(i) $|G(\chi, \psi)|^2 = \sum_{x, y \in E} \chi(x) \psi(x) \overline{\chi(y) \psi(y)} = q - 1 + \sum_{x \neq y \neq 0} \chi(x) \psi(x) \overline{\chi(y) \psi(y)}$
 $= q - 1 + \sum_{x, y \neq 0} \chi\left(\frac{x}{y}\right) \psi(x - y)$
 $= q - 1 + \sum_{\substack{u \neq 1 \\ v \neq 0}} \chi(u) \psi(v)$ (substituting $x = \frac{uv}{u-1}$, $y = \frac{v}{u-1}$)
 $= q - 1 + \left(\sum_{u \neq 1} \chi(u)\right) \left(\sum_{v \neq 0} \psi(v)\right) = q - 1 + (-1)(-1) = q$ (see (ii), (iii)). \square

Now define the **Jacobi sum** of two multiplicative characters $\chi, \chi' \in \widehat{E^\times}$ by

$$J(\chi, \chi') = J(\chi', \chi) = \sum_{\substack{x, y \in E \\ x+y=1}} \chi(x) \chi'(y).$$

Theorem 11.4. Let $\chi, \chi' \in \widehat{E}^\times$ be nontrivial, i.e. $\chi, \chi' \neq \chi_0$. Then

- (i) $J(\chi, \chi') = \begin{cases} -\chi(-1), & \text{if } \chi\chi' = \chi_0, \\ \frac{G(\chi)G(\chi')}{G(\chi\chi')}, & \text{otherwise;} \end{cases}$
- (ii) $J(\chi, \chi_0) = 0$;
- (iii) $J(\chi_0, \chi_0) = q$.

Proof. (ii) and (iii) follow easily using Theorem 11.3(ii). If $\chi\chi' = \chi_0$ then

$$J(\chi, \chi') = \sum_{x \neq 1} \chi(x)\chi^{-1}(1-x) = \sum_{x \neq 1} \chi\left(\frac{x}{1-x}\right) = \sum_{u \neq -1} \chi(u) = -\chi(-1)$$

using Theorem 11.3(ii) and the substitution $x = \frac{u}{u+1}$. Finally if $\chi\chi' \neq \chi_0$ then

$$\begin{aligned} G(\chi)G(\chi') &= \sum_{x, y \in E} \chi(x)\chi'(y)\zeta^{\text{Tr}(x+y)} = \sum_x \chi(x)\chi'(-x) + \sum_{x+y \neq 0} \chi(x)\chi'(y)\zeta^{\text{Tr}(x+y)} \\ &= \chi'(-1) \sum_{x \in E} (\chi\chi')(x) + \sum_{\substack{s, t \in E \\ s \neq 0}} \chi(ts)\chi'((1-t)s)\zeta^{\text{Tr } s} \end{aligned}$$

using the substitution $(x, y) = (ts, (1-t)s)$. Now $\sum_x (\chi\chi')(x) = 0$ since $\chi\chi' \neq \chi_0$, so

$$G(\chi)G(\chi') = \sum_{t \in E} \chi(t)\chi'(1-t) \sum_{s \in E} \chi(s)\chi'(s)\zeta^{\text{Tr } s} = J(\chi, \chi')G(\chi\chi').$$

When χ, χ' and $\chi\chi'$ are all nontrivial, their Gauss sums are nonzero (by Theorem 11.3(i)) and then we can solve for $J(\chi, \chi')$ to obtain the value claimed. \square

An interesting consequence of Theorem 11.4 is that when all of $\chi, \chi', \chi\chi' \in \widehat{E}^\times$ are nonprincipal, $|J(\chi, \chi')| = \sqrt{q}$ using Theorem 11.3(i). An application is

- Corollary 11.5.** (i) Every prime $p \equiv 1 \pmod{4}$ is expressible in the form $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$.
- (ii) Every prime $p \equiv 1 \pmod{3}$ is expressible in the form $p = a^2 - ab + b^2$ with $a, b \in \mathbb{Z}$.

Proof. Here we take $q = p$, so $E = \mathbb{F}_p$.

(i) Suppose $p \equiv 1 \pmod{4}$. Since $|\widehat{E}| = p-1$ is divisible by 4, there exists $\chi \in \widehat{E}$ of order 4; and χ has values in $\mathbb{Z}[i]$ (see Lemma 11.1, where we denoted $\chi = \chi_{\frac{p-1}{4}}$.) Thus $J(\chi, \chi) = a + bi$ for some $a, b \in \mathbb{Z}$. Since χ and χ^2 are nontrivial, $|J(\chi, \chi)|^2 = a^2 + b^2 = p$.

(ii) Now suppose $p \equiv 1 \pmod{3}$. A cubic character $\chi = \chi_{\frac{p-1}{3}} \in \widehat{E}^\times$ has values in $\mathbb{Z}[\omega]$ where $\omega = \zeta_3$. As in (i), we have $J(\chi, \chi) = a + b\omega$ for some $a, b \in \mathbb{Z}$, and $|J(\chi, \chi)|^2 = (a + b\omega)(a + b\bar{\omega}) = a^2 - ab + b^2 = p$. \square

It should be noted that computing $a, b \in \mathbb{Z}$ as in Corollary 11.5 has an efficient algorithmic solution by Fermat's method of descent; however if one only requires an existence proof, then the argument above is hard to beat for conciseness. There is no point in stating Corollary 11.5 more generally for prime powers, since expressing numbers in the form $a^2 + b^2$, or $a^2 - ab + b^2$, reduces to the comparable question for p using elementary arguments. In Corollary 11.5, note the necessity of the assumed congruences for p .

Both the rings $\mathbb{Z}[i]$ ($i = \zeta_4$) and $\mathbb{Z}[\omega]$ ($\omega = \zeta_3$) have unique factorization; see Corollary A3.16. In both these rings, the units are just the roots of unity: $\mathbb{Z}[i]^\times = \langle i \rangle = \{\pm 1, \pm i\}$ and $\mathbb{Z}[\omega]^\times = \langle \zeta_6 \rangle = \{\pm 1, \pm \omega, \pm \omega^2\}$. For a rational prime $p \equiv 1 \pmod{4}$, the expression $p = a^2 + b^2$ is essentially unique: there are in fact eight solutions $(\pm a, \pm b)$, $(\pm b, \pm a)$ corresponding to the factorizations of p as a product of irreducible elements in $\mathbb{Z}[i]$:

$$p = (a+bi)(a-bi) = (-b+ai)(-b-ai) = (-a-bi)(-a+bi) = (b-ai)(b+ai)$$

where all factorizations are obtained from the first one by migration of units.

For a rational prime $p \equiv 1 \pmod{3}$, we have twelve solutions of $p = a^2 - ab + b^2$, all arising from the same factorization of p by migration of units in $\mathbb{Z}[\omega]$:

$$\begin{aligned} p &= (a + b\omega)(a - b - b\omega) = (-b + (a-b)\omega)(-a + (b-a)\omega) = (b-a - a\omega)(b + a\omega) \\ &= (-a - b\omega)(b - a + b\omega) = (b + (b-a)\omega)(a + (a-b)\omega) = (a-b + a\omega)(-b - a\omega). \end{aligned}$$

These are in fact *all* the factorizations of p in the ring $\mathcal{O} = \mathbb{Z}[\omega]$ of Eisenstein integers, since the factors shown are irreducible (since they have norm equal to p , a prime) and \mathcal{O} has unique factorization up to units, of which there are exactly six. The resulting twelve solutions of $p = a^2 - ab + b^2$ are classified according to the pair of residues $(a \pmod{3}, b \pmod{3})$ which evidently cannot be $(0, 0)$, $(1, 2)$ or $(2, 1)$ as these choices yield $a^2 - ab + b^2 \equiv 0 \pmod{3}$. This means that the twelve solutions (a, b) , reduced mod 3, yield each of the six remaining pairs $\pm(1, 1)$, $\pm(1, 0)$, $\pm(0, 1)$ twice. In particular there are two solutions (a, b) , $(a-b, -b)$ which reduce as $(2, 0)$ modulo 3; and we now show that these two solutions are exactly the ones arising from Jacobi sums of cubic characters:

Lemma 11.6. Let $\chi \in \widehat{E}^\times$ be a cubic multiplicative character on a prime field $E = \mathbb{F}_p$ of order $p \equiv 1 \pmod{3}$. Then $J(\chi, \chi) = a + b\omega$ where $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$. Moreover, $(A, B) = (2a - b, \frac{b}{3})$ gives an integer solution of the Diophantine equation $4p = A^2 + 27B^2$ in which $A \equiv 1 \pmod{3}$.

The conditions above essentially characterize $J(\chi, \chi)$ in the following sense: The equation $4p = A^2 + 27B^2$ has just two integer solutions $(A, \pm B)$ satisfying $A \equiv 1 \pmod{3}$; and they arise from $J(\chi, \chi)$ and $J(\bar{\chi}, \bar{\chi})$ as just described, where χ and $\bar{\chi} = \chi^2$ are the two cubic characters of E^\times .

Proof. Under the stated hypotheses,

$$\begin{aligned}
G(\chi)^2 &= G(\chi^2)J(\chi, \chi) \quad (\text{by Theorem 11.4(i)}) \\
&= G(\bar{\chi})J(\chi, \chi) \quad (\text{the inverse of } \chi \text{ is } \bar{\chi} = \chi^2) \\
&= \chi(-1)\overline{G(\chi)}J(\chi, \chi) \quad (\text{by Theorem 11.2(ii)}) \\
&= \overline{G(\chi)}J(\chi, \chi) \quad (\chi(-1) = \pm 1 \text{ but its cube must equal } 1).
\end{aligned}$$

Now multiply both sides by $G(\chi)$ and use Theorem 11.3(i) to get $pJ(\chi, \chi) = G(\chi)^3$. We will reduce both sides of the latter relation (in $\mathcal{O} = \mathbb{Z}[\omega]$) modulo 3, to obtain a relation in the quotient ring $\mathcal{O}/3\mathcal{O}$, a local ring (but not a field) of order 9:

$$pJ(\chi, \chi) = G(\chi)^3 = \left(\sum_{x \in F} \chi(x)\zeta^x \right)^3 \equiv \sum_{x \in F} \chi(x)^3 \zeta^{3x} = -1 \pmod{3}$$

since $\sum_{x \in F} \zeta^{3x} = \sum_{u \in F} \zeta^u = 0$ and $\chi(x)^3 = 0$ or 1 according as $x = 0$ or $x \neq 0$. Since $p \equiv 1 \pmod{3}$, (i) gives $J(\chi, \chi) = a + b\omega \equiv -1 \pmod{3}$, i.e. $a \equiv 1$ and $b \equiv 0 \pmod{3}$. From the defining formula it is clear that $J(\bar{\chi}, \bar{\chi}) = \overline{J(\chi, \chi)} = \overline{a + b\omega} = a - b - b\omega$. Note that the resulting coefficients (a, b) and $(a - b, -b)$ are in fact both of the pairs which reduce to $(2, 0)$ modulo 3 as described.

It is straightforward to check that the substitution $(A, B) = (2a - b, \frac{b}{3})$ transforms an integer solution of $p = a^2 - ab + b^2$ with $a \equiv 2$ and $b \equiv 0 \pmod{3}$ to a solution of $4p = A^2 + 27B^2$ with $A \equiv 1 \pmod{3}$. Conversely, given an integer solution of $A^2 + 27B^2 = 4p$, an easy inspection of this relation modulo 8 shows that A and B must both be odd, so $(a, b) = (\frac{1}{2}(A + 3B), 3B)$ gives a pair of integers congruent to $(2, 0) \pmod{3}$ and satisfying $a^2 - ab + b^2 = p$. \square

We give an application to counting solutions of an equation over a finite field. Theorem 3.6 yields the number of solutions of $x^2 + y^2 = 1$ in a field of odd order; see also Exercise #1. Here we answer the analogous problem for cubes in place of squares.

Theorem 11.7. Given a prime $p \equiv 1 \pmod{3}$, the number of solutions of the equation $x^3 + y^3 = 1$ over \mathbb{F}_p is $p - 2 + A$ where $4p = A^2 + 27B^2$, $A \equiv 1 \pmod{3}$ as in Lemma 11.6.

We remark that for $p \not\equiv 1 \pmod{3}$, the number of solutions of $x^3 + y^3 = 1$ over $E = \mathbb{F}_3$ is exactly p , for rather simple reasons. (If $p = 3$ then $x^3 = x$ for all $x \in E$. If $p \equiv 2 \pmod{3}$ then the map $E \rightarrow E$, $x \mapsto x^3$ is also a permutation of E : it maps $0 \mapsto 0$, and it is an automorphism of the cyclic group E^\times since 3 is relatively prime to $p - 1$.)

Proof of Theorem 11.7. Denote by $\#(x^3 + y^3 = 1)$ the number of solutions of $x^3 + y^3 = 1$ in E . Clearly

$$\#(x^3 + y^3 = 1) = \sum_{a+b=1} \#(x^3 = a)\#(y^3 = b)$$

where $\#(x^3 = a)$ is the number of solutions of $x^3 = a$ in E , and similarly for the other factor. Compare the values of $\#(x^3 = a)$ with the values of a cubic character $\chi = \chi_{\frac{p-1}{3}}$ on E :

$$\#(x^3=a) = \begin{cases} 1, & \text{if } a = 0; \\ 3, & \text{if } a \in E^\times \text{ is a cube;} \\ 0, & \text{if } a \in E^\times \text{ is not a cube;} \end{cases} \quad \chi(a) = \begin{cases} 0, & \text{if } a = 0; \\ 1, & \text{if } a \in E^\times \text{ is a cube;} \\ \omega \text{ or } \bar{\omega}, & \text{if } a \in E^\times \text{ is not a cube.} \end{cases}$$

Observe that $\#(x^3 = a) = 1 + \chi(a) + \overline{\chi(a)} = \chi_0(a) + \chi(a) + \bar{\chi}(a)$ where χ_0 is the trivial multiplicative character, and the two cubic characters are $\chi = \chi_{\frac{p-1}{3}}$ and $\bar{\chi} = \chi_{\frac{2(p-1)}{3}}$. Thus

$$\begin{aligned} \#(x^3 + y^3 = 1) &= \sum_{a+b=1} (\chi_0(a) + \chi(a) + \bar{\chi}(a))(\chi_0(b) + \chi(b) + \bar{\chi}(b)) \\ &= \sum_{i=0}^2 \sum_{j=0}^2 J(\chi^i, \chi^j). \end{aligned}$$

This sum has nine terms, most of which are given by Theorem 11.4:

$$\begin{aligned} J(\chi_0, \chi_0) &= p; & J(\chi_0, \chi) &= J(\chi_0, \bar{\chi}) = J(\chi, \chi_0) = J(\bar{\chi}, \chi_0) = 0; & \text{and} \\ J(\chi, \bar{\chi}) &= J(\bar{\chi}, \chi) = -\chi(-1) = -1 \end{aligned}$$

using again the fact that $\chi(-1) = \pm 1$ but $\chi(-1)^3 = 1$. The remaining two Jacobi sums are given, in the notation of Lemma 11.6, by

$$J(\chi, \chi) + J(\bar{\chi}, \bar{\chi}) = a + b\omega + \overline{a + b\omega} = a + b\omega + (a - b) - b\omega = 2a - b = A.$$

Adding these nine Jacobi sums gives $\#(x^3 + y^3 = 1) = p - 2 + A$. □

Exercises 11.

1. According to Theorem 3.6(i), the number of solutions of $x^2 + y^2 = 1$ in \mathbb{F}_q is $q - (-1)^{\frac{q-1}{2}}$ when q is odd.
 - (a) Give another proof using Jacobi sums, similar to the proof of Theorem 11.7.
 - (b) Explain why the number of solutions of $x^2 + y^2 = 1$ in \mathbb{F}_q is exactly q when q is even.
2. Make a table with five columns, labelled: p , A , B , $p-2+A$, 'solutions'. In the first column, list all primes $p \equiv 1 \pmod{3}$ less than 50. For each p , find the integers $(A, \pm B)$ satisfying $4p = A^2 + 27B^2$ with $A \equiv 1 \pmod{3}$, and list them in columns 2 and 3, entering also the value of $p-2+A$ in column 4. In the last column, list all pairs (x, y) over \mathbb{F}_p satisfying $x^3 + y^3 = 1$ for $x, y \in \mathbb{F}_p$ (note: list all solutions, not just the number of solutions). Count solutions in column 5 in each case and verify that the number of solutions agrees with the expected number from column 4, as predicted by Theorem 11.7. *You may use a computer to perform this exercise.*
3. Let $E = \mathbb{F}_p$, p prime. Choose a multiplicative character $\chi \in \widehat{E^\times}$ of order n ; recall that n divides $p-1$. By definition, $G(\chi) \in \mathbb{Z}[\zeta_n, \zeta_p] = \mathbb{Z}[\zeta_{np}]$. Prove that $G(\chi)^n \in \mathbb{Z}[\zeta_n]$.

Hint: Choose $r \in \{1, 2, 3, \dots, p-1\}$ which is a generator for E^\times . By the Chinese Remainder Theorem, there exists $k \in \mathbb{Z}$ such that $k \equiv 1 \pmod{n}$ and $k \equiv r \pmod{p}$. Now $\mathbb{Q}[\zeta_{np}]$ has a unique automorphism satisfying $\sigma(\zeta_{np}) = \zeta_{np}^k$. Find the fixed field of σ (denoted $\text{Fix}_{\mathbb{Q}[\zeta_{np}]}(\sigma)$ in Appendix A5). Show that $\sigma(G(\chi)) = \chi(r)G(\chi)$ and take n th powers.

12. Zeta Functions and L -Functions

Fix a finite field $F = \mathbb{F}_q$. We will see that characters on F lift naturally to characters on finite extension fields $K \supseteq F$ via the trace and norm maps of the extension. It is natural to ask how the Gauss sums of the lifted characters on K , may be expressed in terms of the Gauss sums of the original characters on F . This is possible using the Hasse-Davenport relations, which we prove in this section. In particular, this generalizes the explicit formula for quadratic Gauss sums over prime fields (Theorem 10.13) to an explicit formula for quadratic Gauss sums over arbitrary finite fields (Corollary 12.11). The key tool in this development is L -functions, which we must first introduce. Because we deal here with L -functions over function fields, students may first want to glance through Appendix A6 where L -functions over number fields are described. If, as we expect, the number field case is more familiar to students, then that Appendix may serve as a bridge to the results in this Section. Yet in no way do we actually require the results of Appendix A6.

Recall that the polynomial ring $\mathcal{O} := F[x]$ is a principal ideal ring; indeed, every nonzero ideal $\mathcal{A} \subseteq \mathcal{O}$ has a unique monic generator. The **norm** of an ideal $\mathcal{A} \subseteq \mathcal{O}$ is the number of cosets: $N(\mathcal{A}) = |\mathcal{O}/\mathcal{A}| = q^n$ assuming \mathcal{A} has a generator of degree n . The norm is multiplicative: $N(\mathcal{A}\mathcal{B}) = N(\mathcal{A})N(\mathcal{B})$ for all ideals $\mathcal{A}, \mathcal{B} \subseteq \mathcal{O}$. Every nonzero prime ideal $\mathfrak{P} \subset \mathcal{O}$ is maximal, and has the form $\mathfrak{P} = (f(x))$ where $f(x) \in \mathcal{O}$ is irreducible; and then the **residue field** $\mathcal{O}/\mathfrak{P} = \mathcal{O}/(f) \cong \mathbb{F}_{q^n}$ where $n = \deg f$.

The **zeta function** of \mathcal{O} is the complex-valued function defined by

$$\zeta_{\mathcal{O}}(s) = \sum_{\mathcal{A}} \frac{1}{N(\mathcal{A})^s}$$

where the sum is over all nonzero ideals $\mathcal{A} \subseteq \mathcal{O}$. (Compare \mathcal{O} with the ring \mathbb{Z} whose nonzero ideals have the form $(n) = n\mathbb{Z}$ for $n \geq 1$, giving the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} |\mathbb{Z}/n\mathbb{Z}|^{-s} = \sum_{n=1}^{\infty} n^{-s}$.) Since nonzero ideals in \mathcal{O} factor uniquely as products of prime ideals, we obtain the factorization

$$\zeta_{\mathcal{O}}(s) = \prod_{\mathfrak{P}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}$$

where \mathfrak{P} ranges over all nonzero prime ideals of \mathcal{O} . This is the **Euler factorization** of $\zeta_{\mathcal{O}}(s)$, valid for exactly the same reasons as for the Riemann zeta function (or for Dedekind zeta functions of more general number fields; see Appendix A6): it is a restatement of the unique factorization property for nonzero ideals, using the fact that the norm is multiplicative.

Now every nonzero ideal $\mathcal{A} \subseteq \mathcal{O}$ has a unique monic generator $f(x) \in \mathcal{O}$; and $N(\mathcal{A}) = q^{\deg f}$. Moreover there are exactly q^n monic polynomials of degree n , so

$$(12.1) \quad \zeta_{\mathcal{O}}(s) = \sum_{n=0}^{\infty} \frac{q^n}{q^{ns}} = \sum_{n=0}^{\infty} q^n z^n = \frac{1}{1 - qz}$$

where we have substituted $z = q^{-s}$. The series converges in the right half-plane $\Re s > 1$, i.e. in the open disk $|z| < \frac{1}{q}$; but by analytic continuation, the function is meromorphic in z with a simple pole at $z = \frac{1}{q}$. The Euler factorization yields

$$(12.2) \quad \zeta_{\mathcal{O}}(s) = \prod_{d=1}^{\infty} \left(1 - \frac{1}{q^{ds}}\right)^{-n_d} = \prod_{d=1}^{\infty} (1 - z^d)^{-n_d}$$

where n_d is the number of prime ideals of norm q^d , i.e. the number of monic irreducible polynomials of degree d ; see Theorem 3.13. Let's verify directly the equality of the two expressions (12.1) and (12.2). Since both series have constant term 1, it suffices to compare their derivatives with respect to z . It is more convenient to use logarithmic differentiation: we apply the operator $Df(z) = z \frac{d}{dz} f(z) = z \frac{f'(z)}{f(z)}$ to both (12.1) and (12.2), and compare the results. For (12.1) we get

$$(12.3) \quad z \frac{d}{dz} \log \left(\frac{1}{1 - qz} \right) = \frac{qz}{1 - qz} = \sum_{n=1}^{\infty} q^n z^n$$

whereas (12.2) yields

$$(12.4) \quad z \frac{d}{dz} \log \prod_{d=1}^{\infty} (1 - z^d)^{-n_d} = -z \frac{d}{dz} \sum_{d=1}^{\infty} n_d \log(1 - z^d) = \sum_{d=1}^{\infty} \frac{dn_d z^d}{1 - z^d} \\ = \sum_{d=1}^{\infty} \sum_{r=1}^{\infty} dn_d z^{rd} = \sum_{n=1}^{\infty} \left(\sum_{1 \leq d|n} dn_d \right) z^n = \sum_{n=1}^{\infty} q^n z^n.$$

Since (12.3) and (12.4) agree, and since (12.1) and (12.2) have the same constant term 1, it follows that (12.1) and (12.2) agree.

Now let λ be a complex-valued multiplicative function defined on the monoid of nonzero ideals of \mathcal{O} . This means that for nonzero ideals $\mathcal{A}, \mathcal{B} \subseteq \mathcal{O}$, we have $\lambda(\mathcal{A}\mathcal{B}) = \lambda(\mathcal{A})\lambda(\mathcal{B})$. We define the **L -function**

$$L_{\lambda}(s) = \sum_{\mathcal{A}} \frac{\lambda(\mathcal{A})}{N(\mathcal{A})^s}$$

where the sum is again over all nonzero ideals $\mathcal{A} \subseteq \mathcal{O}$. Note that for the constant function $\lambda(\mathcal{A}) = 1$, this is just the zeta function. We shall immediately substitute $z = q^{-s}$ as before. In all cases of interest we shall have $|\lambda(\mathcal{A})| \leq 1$; so that by comparison, $L_{\lambda}(s)$ converges in the open disk $|z| < \frac{1}{q}$. The multiplicative property of λ (together with the multiplicative property of the norm, as before) means that $L_{\lambda}(s)$ admits an **Euler factorization**

$$L_{\lambda}(s) = \prod_{\mathfrak{P}} \left(1 - \frac{\lambda(\mathfrak{P})}{N(\mathfrak{P})^s} \right)^{-1}$$

where \mathfrak{P} ranges again over all nonzero prime ideals of \mathcal{O} .

Now each nonzero ideal has a unique monic generator; so it makes sense to write $\lambda(f) = \lambda(\mathcal{A})$ where $\mathcal{A} = (f(x)) \subseteq \mathcal{O}$ and $f(x) \in M$; here we denote by M the monoid of monic polynomials in \mathcal{O} . For $d \geq 0$, denote by $M_d \subset M$ the subset consisting of monic

polynomials of degree d . Also let $P \subset M$ be the set of monic irreducible polynomials; and $P_d = P \cap M_d$ is the set of monic irreducible polynomials of degree d . Thus

$$(12.5) \quad \begin{aligned} L_\lambda(s) &= \sum_{f \in M} \frac{\lambda(f)}{q^{s \deg f}} = \sum_{f \in M} \lambda(f) z^{\deg f} = \sum_{n=0}^{\infty} \sum_{f \in M_n} \lambda(f) z^n \\ &= \prod_{f \in P} \left(1 - \frac{\lambda(f)}{q^{s \deg f}}\right)^{-1} = \prod_{f \in P} (1 - \lambda(f) z^{\deg f})^{-1} = \prod_{d=1}^{\infty} \prod_{f \in P_d} (1 - \lambda(f) z^d)^{-1}. \end{aligned}$$

Applying to (12.5) the differential operator D as above, we obtain

$$(12.6) \quad \begin{aligned} z \frac{d}{dz} \log L_\lambda(s) &= -z \frac{d}{dz} \sum_{d=1}^{\infty} \sum_{f \in P_d} \log(1 - \lambda(f) z^d) = \sum_{d=1}^{\infty} \sum_{f \in P_d} \frac{d \lambda(f) z^d}{1 - \lambda(f) z^d} \\ &= \sum_{d=1}^{\infty} \sum_{f \in P_d} \sum_{r=1}^{\infty} d \lambda(f)^r z^{rd} = \sum_{n=1}^{\infty} \left(\sum_{d|n} d \sum_{f \in P_d} \lambda(f)^{\frac{n}{d}} \right) z^n. \end{aligned}$$

Now how do we come up with suitable choices of λ , other than the constant $\lambda(\mathcal{A}) = 1$? and which choices of multiplicative function are most useful? It is easy to concoct multiplicative functions: simply define $\lambda(f)$ for $f \in P$ arbitrarily, as this will uniquely extend to the entire monoid M using the multiplicative property. And as long as we choose $|\lambda(f)| \leq 1$ for $f \in P$, λ will satisfy this bound for all $f \in M$.

Our interest is in a very special choice of λ , which will greatly simplify the coefficient of z^n in (12.5). To this end, we first fix a multiplicative character $\chi \in \widehat{F^\times}$ and additive character $\psi \in \widehat{F}$ as in Section 11. For an arbitrary monic polynomial

$$f(x) = x^d - a_1 x^{d-1} + a_2 x^{d-2} - \cdots + (-1)^{d-1} a_{d-1} x + (-1)^d a_d \in M_d, \quad d \geq 1,$$

define $\lambda(f) = \chi(a_d) \psi(a_1)$. In particular for $f(x) = x - a \in M_1$, we have $\lambda(f) = \chi(a) \psi(a)$. And of course for the unique monic constant polynomial, we require $\lambda(1) = 1$.

Lemma 12.7. (i) λ is multiplicative.

$$(ii) \text{ Assuming } \chi \text{ and } \psi \text{ are not both trivial, } \sum_{f \in M_n} \lambda(f) = \begin{cases} 1, & \text{if } n = 0; \\ G(\chi, \psi), & \text{if } n = 1; \\ 0, & \text{if } n \geq 2. \end{cases}$$

Proof. (i) Let $f(x) \in M_d$ as above, and $g(x) = x^e - b_1 x^{e-1} + \cdots + (-1)^{e-1} x + (-1)^e \in M_e$. Then

$$f(x)g(x) = x^{d+e} - (a_1 + b_1)x^{d+e-1} + \cdots + (-1)^{d+e} a_d b_e \in M_{d+e}.$$

We have

$$\lambda(f)\lambda(g) = \chi(a_d)\psi(a_1)\chi(b_e)\psi(b_1) = \chi(a_d b_e)\psi(a_1 + b_1) = \lambda(fg).$$

(ii) Since M_1 consists of polynomials of the form $x - a$ for $a \in F$, we have $\sum_{f \in M_1} \lambda(f) = \sum_{a \in F} \chi(a)\psi(a) = G(\chi, \psi)$.

(iii) Write $f(x) = x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n a_n \in M_n$ where $n \geq 2$. Since $\lambda(f)$ does not depend on the coefficients a_2, a_3, \dots, a_{n-1} ,

$$\lambda(f) = \sum_{f \in M_n} \lambda(f) = q^{n-2} \sum_{a_1, a_n \in F} \chi(a_n) \psi(a_1) = q^{n-2} \left(\sum_{a \in F} \chi(a) \right) \left(\sum_{b \in F} \psi(b) \right) = 0$$

since either $\chi \neq \chi_0$ or $\psi \neq \psi_0$. □

Lemma 12.7 gives the coefficient of z^n in the series expansion of (12.5), which therefore (assuming χ and ψ are not both trivial) reduces to a polynomial of degree 1:

$$L_\lambda(s) = 1 - G(\chi, \psi)z.$$

Substituting into (12.6) gives

$$(12.8) \quad \frac{G(\chi, \psi)z}{1 + G(\chi, \psi)z} = \sum_{n=1}^{\infty} (-1)^{n-1} G(\chi, \psi)^n z^n = \sum_{n=1}^{\infty} \left(\sum_{d|n} d \sum_{f \in P_d} \lambda(f)^{\frac{n}{d}} \right) z^n.$$

There is a very straightforward interpretation of the coefficients of z^n on the right. For each finite extension $K = \mathbb{F}_{q^n}$, $[K : F] = n$, the characters $\chi \in \widehat{F}^\times$ and $\psi \in \widehat{F}$ lift to characters $\chi^K \in \widehat{K}^\times$ and $\psi^K \in \widehat{K}$ defined by

$$\chi^K(a) = \chi(\mathrm{N}_{K/F} a), \quad \psi^K(a) = \psi(\mathrm{Tr}_{K/F} a) \quad \text{for } a \in K.$$

Note that χ^K is multiplicative since it is a composite of two multiplicative functions (Theorem A1.7); similarly ψ^K is an additive character. We will assume that $\chi \neq \chi_0$. In the Gauss sum

$$(12.9) \quad G(\chi^K, \psi^K) = \sum_{a \in K} \chi^K(a) \psi^K(a) = \sum_{0 \neq a \in K} \chi^K(a) \psi^K(a)$$

we partition the terms according to the minimal polynomial $f(x)$ of $a \in K^\times$ over F , grouping together all terms arising from roots of $f(x)$. Each such polynomial has $d = \deg f = [F[a] : F]$ dividing $n = [K : F]$; and in the intermediate field $E := F[a]$ we obtain the splitting

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_d), \quad a \in \{r_1, r_2, \dots, r_d\} \subseteq E.$$

Evidently

$$f(x) = x^d - (\sum_i r_i) x^{d-1} + \cdots + (-1)^d (\prod_i r_i)$$

and so

$$\begin{aligned} \lambda(f)^{\frac{n}{d}} &= \chi(\prod_i r_i)^{\frac{n}{d}} \psi(\sum_i r_i)^{\frac{n}{d}} \\ &= \chi((\mathrm{N}_{E/F} a)^{\frac{n}{d}}) \psi\left(\frac{n}{d} \mathrm{Tr}_{E/F} a\right) \quad (\text{by Theorem A5.13}) \\ &= \chi(\mathrm{N}_{K/F} a) \psi(\mathrm{Tr}_{K/F} a) \quad (\text{by Corollary A1.10}) \\ &= \chi^K(a) \psi^K(a). \end{aligned}$$

Moreover all algebraic conjugates of a (the d roots of $f(x)$) all contribute this same term to the sum. Thus the coefficient of z^n on the right side of (12.8) is

$$\sum_{d|n} d \sum_{f \in P_d} \lambda(f)^{\frac{n}{d}} = \sum_{a \in K} \chi^K(a) \psi^K(a) = G(\chi^K, \psi^K).$$

Now comparing coefficients in (12.8) gives $G(\chi^K, \psi^K) = (-1)^{n-1} G(\chi, \psi)^n$. This is known as the **Hasse-Davenport lifting relation**, which can also be rewritten slightly as

Theorem 12.10 (Hasse-Davenport). Let χ and ψ be nontrivial where $F = \mathbb{F}_q$. For each finite extension $K = \mathbb{F}_{q^n} \supseteq F$, denote by $\chi^K \in \widehat{K^\times}$ and $\psi^K \in \widehat{K}$ the characters obtained by lifting. Then

$$-G(\chi^K, \psi^K) = (-G(\chi, \psi))^n.$$

Lang [L1] defines $G(\chi, \psi)$ to be $-\sum_a \chi(a)\psi(a)$ instead of $\sum_a \chi(a)\psi(a)$, thereby simplifying this formula and some others. This seems such a natural choice that I was tempted to follow it in these notes; but ultimately I settled on the choice of most authors for the sake of consistency.

Now in the case p is odd, the quadratic character of $F = \mathbb{F}_p$ is $\chi(a) = \left(\frac{a}{p}\right)$, this being the unique character $\chi \in \widehat{F^\times}$ of order 2. Not surprisingly, the character $\chi^K \in \widehat{K^\times}$ obtained by lifting, is nothing other than the quadratic character of K , this being its unique multiplicative character of order 2. We check that

$$\chi^K(a) = \chi(N_{K/F}(a)) \equiv (a^{\frac{q-1}{p-1}})^{\frac{p-1}{2}} = a^{\frac{q-1}{2}} \pmod{p}$$

which is indeed the quadratic character on K ; see also Exercise #3.3. As a special case of Theorem 12.10, we have

Corollary 12.11. Let $\chi \in \widehat{K^\times}$ be the quadratic character on a finite field of odd order $q = p^n$. Then $G(\chi) = \begin{cases} (-1)^{n-1} \sqrt{q}, & \text{if } p \equiv 1 \pmod{4}; \\ (-i)^{n+2} \sqrt{q}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$

Proof. On $F = \mathbb{F}_p$, the additive character $\psi_1(a) = \zeta^a$ lifts to $\psi^K(a) = \zeta^{\text{Tr}_{K/F} a}$. By Theorem 12.10, $G(\chi^K) = G(\chi^K, \psi^K) = (-1)^{n-1} G(\chi, \psi)^n = (-1)^{n-1} G(\chi)^n$. Now the result follows from Theorem 10.13. \square

Exercises 12.

1. According to the Kronecker-Weber Theorem (see Section 4), every abelian extension of \mathbb{Q} is contained in a cyclotomic extension. In particular, every quadratic extension of \mathbb{Q} should be contained in a cyclotomic extension. Here we verify this fact without using the Kronecker-Weber Theorem. Let $F \supset \mathbb{Q}$ be a quadratic field extension; this is, $[F : \mathbb{Q}] = 2$.
 - (a) Show that $F = \mathbb{Q}[\sqrt{d}]$ for some integer $d \not\equiv 0 \pmod{4}$. (*Hint:* Choose $\theta \in F$, $\theta \notin \mathbb{Q}$, and let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of θ over \mathbb{Q} . Consider the discriminant of f .)
 - (b) If d is as in (a), use Corollary 12.11 to show that $\sqrt{d} \in \mathbb{Q}[\zeta_n]$ for some positive integer n . Verify this first in the case that d is a prime power; then extend to the general case $d \not\equiv 0 \pmod{4}$.

13. Exponential Sums

Consider a prime field $F = \mathbb{F}_p$. Generalizing slightly the definition of a Gauss sum, it would be natural to consider sums of the form

$$\sum_{a \in F} \chi(a) \psi(f(a)) = \sum_{a \in F} \chi(a) \zeta^{f(a)}$$

for an arbitrary function $f : F \rightarrow F$. As we shall soon see, for quadratic polynomials $f(x)$ the corresponding sums are already expressible in the language of Gauss sums. For more general functions $f : F \rightarrow F$ there is much more to be said; and the case where χ is trivial is already sufficiently interesting. This leads to the definition of exponential sums given below; and it is worth keeping in mind that both Gauss sums and exponential sums are special cases of sums having the form suggested above. While neither type of sum (Gauss or exponential) is a generalization of the other, we shall see that the two types of sum coincide in the quadratic case.

For an arbitrary function $f : F \rightarrow F$, $F = \mathbb{F}_p$, $\zeta = \zeta_p = e^{2\pi i/p}$, we define the exponential sum of f as

$$S_f := \sum_{a \in F} \zeta^{f(a)} \in \mathbb{Z}[\zeta].$$

For more general finite fields $E = \mathbb{F}_q$, $q = p^e$, we must compose with the trace map $\text{Tr} = \text{Tr}_{E/F} : E \rightarrow F$. Recall that this is the F -linear map defined by

$$\text{Tr } a = a + a^p + a^{p^2} + \cdots + a^{p^{e-1}}.$$

Since $\text{Tr } a \in \mathbb{F}_p$, we are able to meaningfully define the **exponential sum** of f as

$$S_f = S_{f(x)} := \sum_{a \in E} \zeta^{\text{Tr } f(a)} \in \mathbb{Z}[\zeta],$$

noting that values of S_f are still in the same ring $\mathbb{Z}[\zeta]$, $\zeta = \zeta_p$ as before. Of course S_f depends really only on the multiset of values of f rather than on f itself: in general there

will be many functions $g : E \rightarrow E$ such that f and g take each value in E the same number of times, in which case $S_g = S_f$. In particular, there are $q!$ permutations of E , all having the same exponential sum $S_f = 0$, this being a consequence of the relation $\sum_{a \in E} \zeta^{\text{Tr } a} = 0$, which remains valid after an arbitrary permutation of terms in the sum. We note that (ii) only holds in the case of prime fields.

Lemma 13.1. For exponential sums over a field of order q , we have

- (i) $|S_f| \leq q$; and equality holds iff f is a constant function.
- (ii) Suppose that $q = p$. Then any two functions $f, g : F \rightarrow F$ have the same exponential sum $S_f = S_g$ iff f and g have the same multiset of values (i.e. for every $b \in E$, the equation $f(x) = a$ has the same number of solutions as the equation $g(x) = a$). In particular, $S_f = 0$ iff $f : F \rightarrow F$ is a permutation of F .

Proof. Conclusion (i) is a simple application of the triangle inequality. In (ii), the argument above proves the ‘ \Leftarrow ’ in both ‘iff’ statements; and the ‘ \Rightarrow ’ direction in both statements follows using the fact that $\Phi_p(x) = 1 + x + x^2 + \dots + x^{p-1}$ is the minimal polynomial of ζ over F . \square

It is worth keeping in mind that a ‘random’ function $f : F \rightarrow F$ is expected to have $|S_f| \approx \sqrt{q}$, which is rather smaller than the upper bound of Lemma 13.1(i). This follows from

$$|S_f|^2 = S_f \overline{S_f} = \sum_{a \in F} \zeta^{\text{Tr } f(a)} \sum_{b \in F} \zeta^{-\text{Tr } f(b)} = \sum_{a, b \in F} \zeta^{\text{Tr}[f(a) - f(b)]} = q + \sum_{a \neq b} \zeta^{\text{Tr}[f(a) - f(b)]} \approx q,$$

assuming the values of $\text{Tr } f(a)$ are uniformly distributed in \mathbb{F}_p , leading to widespread cancellation of terms in the latter sum. The argument in fact shows (using linearity of expectation) that for a random walk consisting of n unit steps in the plane, the steps being taken randomly and independently from some distribution which is balanced (the expected step being the zero vector), the expected square of the total distance travelled is n ; and thus the RMS (root mean square) distance travelled is \sqrt{n} . This argument *does not* say that the expected length of a random walk is \sqrt{n} (since the squaring function is nonlinear); nevertheless the approximation $|S_f| \approx \sqrt{q}$ is a handy gauge against which to compare $|S_f|$ for those functions f which we encounter. Similar heuristics may be applied to estimating more general sums of the form $\sum_{a \in F} \chi(g(a))\psi(f(a))$.

The single most important result on exponential sums is

Theorem 13.2. Suppose $f : E \rightarrow E$ is represented by a polynomial in $E[x]$ of degree $d \geq 1$, where d is not divisible by p . Then $|S_f| \leq (d-1)\sqrt{q}$.

This bound, which we refer to as **Weil's bound**, also known as the **Hasse-Davenport-Weil bound**, is actually the result of several 20th century mathematicians including André Weil. The first complete proof of this bound relies on Pierre Deligne's work on the Weil conjectures, work completed in 1973 and for which he received the Fields Medal in 1978. While the Weil conjectures are quite deep and far-reaching, today we have proofs by more elementary methods; see [LN], [Sc]. We will not present the full proof of Weil's bound; but in Section 17 we present some of the key elements in an 'elementary' proof. We mention that Weil's bound extends also to Galois rings; and that we [MSW] have applied Weil's bound to eigenvalues of algebraically defined graphs, both for finite fields and for Galois rings.

Note the obvious necessity of $d \geq 1$ in Weil's bound; and the necessity of the hypothesis $p \nmid d$ is discussed in Exercise #2. Weil's bound is of course useless for larger values $d \geq 1 + \sqrt{q}$, since in that case it is weaker than the trivial bound of Lemma 13.1(i). In applications of Weil's bound, the reader is reminded that every function $f : E \rightarrow E$ is representable as a polynomial of degree $d \leq q-1$, simply using interpolation. In general, the strength of Weil's bound depends on the particular choice of p -th root of unity ζ (recall that one has $\phi(p) = p-1$ choices for ζ). Of course for $d = 1$, Weil's bound holds with equality (since polynomial maps of degree 1 are permutations; see Lemma 13.1(ii)). It is not hard to show that equality also holds for quadratic polynomials:

Theorem 13.3. Consider an arbitrary quadratic polynomial $f(x) = ax^2 + bx + c \in E[x]$, $a \neq 0$ where $E = \mathbb{F}_q$, $q = p^e$, p an odd prime, $e \geq 1$. Writing $d = \frac{1}{4a}(b^2 - 4ac)$, we have

- (i) $S_f = \chi(a)\zeta^{-\text{Tr } d}G(\chi)$ where χ is the quadratic character on E ($\chi(a) = 0, 1, -1$ for $a = 0$, nonzero square, nonsquare respectively) and $S_{x^2} = G(\chi)$ is the quadratic Gauss sum. In particular, $|S_f| = \sqrt{q}$.
- (ii) If $q = p$ and $\zeta = e^{2\pi i/p}$ then

$$S_f = \begin{cases} \left(\frac{a}{p}\right)\zeta^{-d}\sqrt{p}, & \text{if } p \equiv 1 \pmod{4}; \\ i\left(\frac{a}{p}\right)\zeta^{-d}\sqrt{p}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Recall that the generalization of (ii) for arbitrary odd q , giving the exact value of the quadratic Gauss sum $G(\chi)$, was found at the end of Section 12.

Proof of Theorem 13.3. The quadratic Gauss sum is

$$G(\chi) = \sum_{x \in E} \chi(x)\zeta^{\text{Tr } x} = \sum_{\chi(y)=1} \zeta^{\text{Tr } y} - \sum_{\chi(y)=-1} \zeta^{\text{Tr } y} = 1 + 2 \sum_{\chi(y)=1} \zeta^{\text{Tr } y} = -1 - 2 \sum_{\chi(y)=-1} \zeta^{\text{Tr } y}$$

since $0 = \sum_{y \in E} \zeta^{\text{Tr } y} = 1 + \sum_{\chi(y)=1} \zeta^{\text{Tr } y} + \sum_{\chi(y)=-1} \zeta^{\text{Tr } y}$. Now if $f(x) = ax^2$, $\chi(a) = 1$ then

$$S_f = \sum_{x \in E} \zeta^{\text{Tr}(ax^2)} = 1 + 2 \sum_{\chi(y)=1} \zeta^{\text{Tr } y} = G(\chi)$$

whereas if $f(x) = ax^2$, $\chi(a) = -1$ then

$$S_f = \sum_{x \in E} \zeta^{\text{Tr}(ax^2)} = -1 - 2 \sum_{\chi(y)=-1} \zeta^{\text{Tr} y} = -G(\chi).$$

In either case, we have $S_{ax^2} = \chi(a)G(\chi)$.

In the general case, $f(x) = ax^2 + bx + c = a(x + \frac{b}{2a})^2 - d = g(x + \frac{b}{2a}) - d$ where $g(x) = ax^2$ and $d = \frac{1}{4a}(b^2 - 4ac)$. Substituting $u = x + \frac{b}{2a}$, we get

$$S_f = \sum_{x \in E} \zeta^{\text{Tr} f(x)} = \sum_{u \in E} \zeta^{\text{Tr}(g(u)-d)} = \zeta^{-\text{Tr} d} S_g = \chi(a) \zeta^{-\text{Tr} d} G(\chi).$$

The remaining assertions follows from Theorems 11.3(i) and 10.13. □

In the case of prime fields $E = \mathbb{F}_p$, we have already observed that those functions $f : E \rightarrow E$ attaining $|S_f| = 0$ are just the permutations of E . Similarly, Theorem 13.3 admits a converse which characterizes those functions attaining Weil's bound $|S_f| = \sqrt{q}$ as exactly the quadratic polynomials, or permuted versions thereof (via Lemma 13.1(ii)):

Theorem 13.4 (Cavior [Ca]). Let $f : F \rightarrow F$ where $F = \mathbb{F}_p$, p an odd prime. Then $|S_f| = \sqrt{p}$ iff f has the same multiset of values as a quadratic polynomial.

Proof. If f has the same multiset of values as a quadratic polynomial, then $|S_f| = \sqrt{p}$ by Lemma 13.1(ii) and Theorem 13.3.

Conversely, suppose $|S_f| = \sqrt{p}$, so that $S_f \overline{S_f} = p = S_g \overline{S_g}$ where $g(x) = x^2$. So the principal ideals in $\mathcal{O} = \mathbb{Z}[\zeta]$ generated by the algebraic integers $\alpha := S_f$ and $\beta := S_g$ satisfy $(\alpha)(\overline{\alpha}) = (\beta)(\overline{\beta}) = (p) = (\varepsilon)^{p-1}$ where the ideal $(\varepsilon) = (1 - \zeta) \subset \mathcal{O}$ is the only distinct prime factor of (p) ; see Theorem 4.4. By unique factorization of ideals we therefore have $(\alpha) = (\varepsilon)^r$ and $(\overline{\alpha}) = (\varepsilon)^s$ for some nonnegative integers satisfying $r + s = p - 1$. Since $N_{\mathbb{Q}[\zeta]/\mathbb{Q}}(\alpha) = N_{\mathbb{Q}[\zeta]/\mathbb{Q}}(\overline{\alpha})$, we have $r = s$; so $(\alpha) = (\overline{\alpha}) = (\varepsilon)^{(p-1)/2}$. The same argument applies to β , giving $(\beta) = (\varepsilon)^{(p-1)/2} = (\alpha)$. Thus α and β are associates, and $\alpha = u\beta$ for some unit $u \in \mathcal{O}^\times$. Since $|\alpha| = |\beta| = \sqrt{p}$, we obtain $|u| = 1$. Moreover for every $\sigma \in \text{Aut } \mathbb{Q}[\zeta]$, Theorem 4.1 gives

$$|\sigma(u)|^2 = \sigma(u) \overline{\sigma(u)} = \sigma(u) \sigma(\overline{u}) = \sigma(u\overline{u}) = \sigma(1) = 1$$

so $|\sigma(u)| = 1$. By Theorem 4.10, u is a root of unity. Now the only roots of unity in $\mathbb{Q}[\zeta]$ are $\pm 1, \pm \zeta, \dots, \pm \zeta^{p-1}$ by Theorem 4.2, so we have two cases. If $u = \zeta^k$, $k \in \{0, 1, 2, \dots, p-1\}$, then $S_f = \zeta^k S_g = S_h$ where $h(x) = x^2 + k$. By Lemma 13.1(ii), f has the same multiset of values as the quadratic polynomial $h(x) = x^2 + k$ and we are done.

Otherwise $u = -\zeta^k$, $k \in \{0, 1, 2, \dots, p-1\}$ and by Theorem 13.3, the polynomial $h(x) = \eta x^2 + k$ has exponential sum $S_h = -\zeta^k S_g$ provided $\eta \in E$ is a nonsquare. Once again, $S_f = u S_g = S_h$ so by Lemma 13.1(ii), f has the same multiset of values as h . \square

Cavior's Theorem shows that exponential sums provide a characterization of quadratic polynomials over $F = \mathbb{F}_p$, p prime. Some further characterizations of polynomials of degree 0, 1 and 2, also using exponential sums, are given in Theorems 13.5, 13.11, 13.12 and 14.2 below. Applications of these results will be given in Sections 14, 15 and 16.

Theorem 13.5 [M3]. Let $f : F \rightarrow F$ where $F = \mathbb{F}_p$, p an odd prime. Suppose there exists a real constant $\kappa > 0$ such that for all $c \in F$, the exponential sum of the function $x \mapsto f(x) + cx$ satisfies $|S_{f(x)+cx}| \in \{0, \kappa\}$. Then either

- (a) f is quadratic and $|S_{f(x)+cx}| = \sqrt{p}$ for all $c \in F$, or
- (b) f is constant or linear, i.e. $f(x) = a_1 x + a_0$ for some $a_0, a_1 \in F$ and

$$|S_{f(x)+cx}| = \begin{cases} 0, & \text{if } c \neq -a_1; \text{ or} \\ p, & \text{if } c = -a_1. \end{cases}$$

Proof. Let $\zeta = \zeta_p$. For each $c \in F$, define $\alpha_c \in \mathbb{C}$ by

$$\alpha_c = \begin{cases} \kappa^{-1} S_{f(x)+cx}, & \text{if } S_{f(x)+cx} \neq 0; \\ 1, & \text{if } S_{f(x)+cx} = 0 \end{cases}$$

so that $|\alpha_c| = 1$ for all c . Consider the complex $p \times p$ matrix

$$M = [\overline{\alpha_c} \zeta^{xy+f(y)} : x, y \in F].$$

A straightforward computation yields $MM^* = pI_p$ where M^* is the conjugate transpose of M and I_p is the $p \times p$ identity matrix. Equivalently, $\frac{1}{\sqrt{p}}M$ is unitary. Now M is diagonalizable and each of its eigenvalues has absolute value \sqrt{p} .

Let $\mathbf{1} \in \mathbb{C}^p$ be the column vector of 1's. The hypothesis says that the vector $M\mathbf{1}$ has k entries equal to κ , and $p-k$ entries equal to zero, where k is the number of $c \in F$ such that $|S_{f(x)+cx}| = \kappa$. Now

$$k\kappa^2 = \|M\mathbf{1}\|^2 = p\|\mathbf{1}\|^2 = p^2.$$

In particular, $k \geq 1$ and so $\kappa = |S_{f(x)+cx}|$ for some $c \in F$. Since $\kappa^2 = S_{f(x)+cx} \overline{S_{f(x)+cx}} \in \mathbb{Z}[\zeta]$, κ itself must be an algebraic integer. However, $\kappa = \frac{p^2}{k} \in \mathbb{Q}$; so by Theorem A3.2(ii), $\kappa \in \mathbb{Z}$ and $k \in \{1, p\}$.

If $k = p$ then $|S_{f(x)+cx}| = \sqrt{p}$ for all $c \in F$ and so by Theorem 14.2, our conclusion (a) holds. Otherwise we have $k = 1$, and $|S_{f(x)-a_1 x}| = \kappa = p$ for some $a_1 \in F$. This means that we have a constant function $f(x) - a_1 x = a_0 \in F$, so (b) holds. \square

The next two technical lemmas will be required for our main results. For every function $f : F \rightarrow F$, we define

$$A_f = \{a \in F : S_{f(x)+ax} \neq 0\}.$$

Lemma 13.6 ([M3]). Suppose $|A_f| \leq \frac{1}{2}(p+1)$. Then $|A_f| = 1$, and f is either constant or linear; i.e. $f(x) = a_1x + a_0$ for some $a_0, a_1 \in F$.

Proof. By definition, $a \in A_f$ iff there exist distinct $x, y \in F$ such that $f(x)+ax = f(y)+ay$. Thus the subset $-A_f = \{-a : a \in A_f\}$ coincides with the set of all slopes of secants to the graph of f in F^2 , i.e. the set of all values of the difference quotient $(f(y) - f(x))/(y - x)$ for $x \neq y$ in F . The result follows by a theorem of Rédei [Re]; see also [Bl], [LS]. \square

Lemma 13.7 ([M3]). Let $F = \mathbb{F}_p$, p prime, and suppose $g : F \rightarrow F$ is a non-constant function satisfying $|S_{x^2+cg(x)}| = \sqrt{p}$ for all $c \in F$. Then g is a permutation of F . If moreover $g(0)=0$ and $g(1)=1$, then $g(x) = \pm x$ for all $x \in F$.

Proof. We use geometric terminology for the affine plane F^2 , which has p vertical lines of the form $x = a$ ($a \in F$) and p^2 non-vertical lines of the form $y = mx + b$ ($m, b \in F$). Consider the point set $\mathcal{O} = \{(g(t), t^2) : t \in F\} \subset F^2$. We will soon show that \mathcal{O} consists of p^2 distinct points. First observe that if the equation $t^2 = mg(t) + b$ has more than two solutions for $t \in F$, then the function $h(t) = t^2 - mg(t)$ attains the value b more than twice, contrary to Cavior's Theorem 13.4. This shows that

$$(13.8) \quad \text{for all } m, b \in F, \text{ there are at most two values of } t \in F \text{ such that the point } (g(t), t^2) \text{ lies on the line } y = mx + b.$$

Next we show that

$$(13.9) \quad \mathcal{O} \text{ consists of } p^2 \text{ distinct points.}$$

If $(g(t_1), t_1^2) = (g(t_2), t_2^2)$, $t_1 \neq t_2$, then $t_2 = -t_1 \neq 0$. In this case, since g is not constant, there exists $t_3 \in F$ such that $g(t_3) \neq g(t_1)$. Let $m = (t_3^2 - t_1^2)/(g(t_3) - g(t_1))$, $b = t_1^2 - mg(\pm t_1) = t_3^2 - mg(t_3)$; then the line $y = mx + b$ passes through $(g(t_i), t_i^2)$ for $i = 1, 2, 3$, contrary to (13.8). This proves (13.9).

Now let $\ell \subset F^2$ be any line, vertical or non-vertical. By (13.8), $|\ell \cap \mathcal{O}| = 0, 1$ or 2 ; and we call ℓ a **passant**, **secant** or **tangent** accordingly. Each point $P \in \mathcal{O}$ lies on exactly $p+1$ lines, of which $p-1$ are secants, and so P lies on exactly two tangents, one of which (we claim) must be vertical. For each $m \in F$, the function $h(t) = t^2 - mg(t)$ attains some

value $b \in F$ exactly once, and each other value in F either 0 or two times, again by Cavior's Theorem; so among the p lines of slope m , exactly one (the line $y = mx + b$) is a tangent line. Since there are p choices of m , there are exactly p non-vertical tangents; hence the remaining p tangents must be vertical. Thus

(13.10) each vertical line is tangent to \mathcal{O} . That is, g is a permutation of F .

Thus \mathcal{O} is the graph Γ_f of a function $f : F \rightarrow F$ satisfying the hypotheses of Segre's Theorem 3.14. We conclude that $\mathcal{O} = \{(x, f(x)) : x \in F\}$ and $f(x) = ax^2 + bx + c$ for some $a, b, c \in F$ with $a \neq 0$.

Henceforth we assume that $g(0) = 0$ and $g(1) = 1$, so that $(0, 0), (1, 1) \in \mathcal{O}$. Also the only point $(g(x), x^2) \in \mathcal{O}$ with second coordinate zero is $(0, 0)$; so the x -axis is tangent to \mathcal{O} , forcing $f(x) = x^2$. The result follows. \square

Theorem 13.11 ([M3]). Let $f_1, f_2 : F \rightarrow F$ be linearly independent functions satisfying $f_i(0) = 0$, and suppose that $|S_{af_1+bf_2}| \in \{0, \sqrt{p}, p\}$ for all $a, b \in F$. Then there exists a permutation $\sigma : F \rightarrow F$ and constants $a_i, b_i \in F$ such that $f_i(x) = a_i\sigma(x)^2 + b_i\sigma(x)$, $i = 1, 2$.

Proof. If $|S_{af_1+bf_2}| = p$ then $af_1 + bf_2$ is constant; and since $f_i(0) = 0$, this means $af_1 + bf_2 = 0$. Since f_1 and f_2 are linearly independent, this forces $a = b = 0$. Thus $|S_{af_1+bf_2}| \in \{0, \sqrt{p}\}$ whenever $(a, b) \neq (0, 0)$.

Consider the case that f_2 is a permutation. In this case we may assume $f_2(x) = x$; otherwise replace f_i by $f_i \circ f_2^{-1}$ for $i = 1, 2$. Now $|S_{f_1(x)+bx}| \in \{0, \sqrt{p}\}$ for all $b \in F$; so by Theorem 13.5, $f_1(x) = a_1x^2 + b_1x$ for some $a_1, b_1 \in F$ with $a_1 \neq 0$. The result follows in this case.

Now if the two-dimensional space $\langle f_1, f_2 \rangle_F$ of functions $F \rightarrow F$ contains a permutation, then by change of basis we reduce to the previous case. We may therefore assume $\langle f_1, f_2 \rangle_F$ contains no permutation, i.e. $|S_{af_1+bf_2}| = \sqrt{p}$ for all $(a, b) \neq (0, 0)$. In particular $|S_{f_1}| = \sqrt{p}$ so by Cavior's Theorem 13.4, there exists a permutation $\sigma : F \rightarrow F$ such that $f_1(x) = a_1\sigma(x)^2 + b_1\sigma(x)$, $a_1 \neq 0$; moreover $\sigma(0) = 0$ (thus ensuring the value $f_1(0) = 0$). Furthermore, there is no loss of generality in assuming that $\sigma(x) = x$ and $a_1 = 1$; so $|S_{x^2+b_1x+bf_2(x)}| = \sqrt{p}$ for all $b \in F$. Define $h(x) = f_2(x - \frac{b_1}{2}) - f_2(-\frac{b_1}{2})$; then $|S_{x^2+bh(x)}| = |S_{x^2+b_1x+bf_2(x)}| = \sqrt{p}$ for all $b \in F$, so $h : F \rightarrow F$ is bijective by Lemma 13.7. This means that f_2 is a permutation after all. \square

In Section 16 we will also require one more such characterization of polynomials of small degree:

Theorem 13.12 ([M3]). Let $f : F \rightarrow F$ where $F = \mathbb{F}_p$, and let $a \in F$ be a nonzero constant. Suppose that $|S_{ax^2+bx+cf(x)}| = \sqrt{p}$ for all $b, c \in F$. Then $f(x) = mx + d$ for some $m, d \in F$.

Proof. By hypothesis,

$$\begin{aligned} p &= \left| \sum_{x \in F} \zeta^{ax^2+bx+cf(x)} \right|^2 = \sum_{x, y \in F} \zeta^{a(x^2-y^2)+b(x-y)+c(f(x)-f(y))} \\ &= \sum_{y, t \in F} \zeta^{2aty+t^2+bt+c(f(y+t)-f(y))} \end{aligned}$$

for all $b, c \in F$. Multiply both sides by ζ^{-b} and sum over $b \in F$ to obtain

$$(13.13) \quad \sum_{y \in F} \zeta^{2ay+a+c(f(y+1)-f(y))} = 0 \text{ for all } x \in F.$$

Now suppose the desired conclusion fails, i.e. f is not representable as a polynomial of degree ≤ 1 ; we seek a contradiction. Evidently the first-order difference of f is not constant, so there exists $x \in F$ such that

$$f(x+1) - f(x) \neq m$$

where $m = f(1) - f(0)$. Clearly $x \neq 0$. Set

$$c = \frac{2ax}{m - [f(x+1) - f(x)]}$$

and check that the exponent in (13.13) takes the same value for $y = 0$ and for $y = x$. However, the only way for the exponential sum (13.13) to vanish is for the exponent to have distinct values as y varies over F , which is the desired contradiction. \square

Exercises 13.

1. Give a direct proof (i.e. without using Gauss sums) that the exponential sum S_f for $f(x) = ax^2$ on $E = \mathbb{F}_q$, q odd, $a \neq 0$, has modulus $|S_f| = \sqrt{q}$. (*Hint:* Expand $|S_f|^2 = S_f \overline{S_f}$ as a double sum, and use orthogonality of additive characters.)
2. Let $E = \mathbb{F}_q$ where $q = p^e$, p prime, $e \geq 2$; and consider the function $f : E \rightarrow E$, $a \mapsto a^p - a$. Evaluate S_f and find conditions under which Weil's bound of Theorem 13.2 fails. This points to the necessity of the hypothesis $\gcd(d, q) = 1$ in that result.
3. Show by example the necessity of the hypothesis that p is prime in Cavior's Theorem 13.4. (*Hint:* Take $E = \mathbb{F}_9 = \mathbb{F}_3[i]$ where $i^2 = -1$. If $g(x) = x^2$ then $|S_g| = \sqrt{9} = 3$. Find three terms in the sum S_g of the form $\zeta^0 + \zeta^1 + \zeta^2 = 0$ and modify just the three corresponding values of $g(x)$ to create a new function f with the same three terms in its exponential sum, so that $S_f = S_g$. With some care, you can arrange that f takes on some value more than twice, so f has a different multiset of values from any quadratic polynomial.)

14. Affine Planes

An **affine plane of order n** is an incidence system of n^2 points and $n(n+1)$ lines such that

- Each line has exactly n points;
- Any two distinct points lie on exactly one line;
- Given any line ℓ and any point P not on ℓ , there is exactly one line m through P having no point in common with ℓ .

Now in an affine plane, we say two lines ℓ and m are **parallel** (denoted $\ell \parallel m$) if they are either the same line, or they are disjoint (i.e. have no points in common). The axioms above say that parallelism of lines is an equivalence relation (and in particular if $\ell_1 \parallel \ell_2$ and $\ell_2 \parallel \ell_3$, then $\ell_1 \parallel \ell_3$). Each parallel class of lines consists of n lines of size n , constituting a partition of the n^2 points. Each point lies on exactly $n+1$ lines, one from each parallel class. If two lines are not parallel, then they meet in exactly one point.

The **classical affine plane** of order q (a prime power) is the plane coordinatized by $F = \mathbb{F}_q$ in the usual way: Take points to be the q^2 ordered pairs $(x, y) \in F^2$. There are $q(q+1)$ lines $\ell_{m,h}$ where $m \in F \cup \{\infty\}$, $h \in F$, defined as follows:

- ‘Vertical’ lines are point sets of the form $\ell_{\infty,k} := \{k\} \times F = \{(k, y) : y \in F\}$ for $k \in F$. Each such line may also be specified also by its equation $x = k$.
- ‘Nonvertical’ lines are point sets of the form $\ell_{m,h} := \{(x, mx+h) : x \in F\}$ where $m, h \in F$. Each such line is also specified by its equation $y = mx+h$.

One readily checks that this structure satisfies the properties required of an affine plane listed above. So for each prime power n , there is at least one plane of order n .

There exist many constructions of finite affine planes which are not isomorphic to the classical planes constructed above. However, all known finite planes have prime power order; and this has encouraged some to conjecture that every finite affine plane must have prime power order. Take heed, however, of The Streetlight Effect (Section 9): it may well be that the planes of prime order are the only ones known, simply because they are the easiest ones to find.

The smallest non-classical planes have order 9; and in fact there are seven affine planes of order 9 up to isomorphism, including the classical plane. (See [HP], [M4] for a general introduction to affine and projective planes. Those familiar with the usual process of projective completion will recognize that every affine plane of order n also yields a projective plane of order n , but we will stick to the affine description here.)

One hopeful scheme for constructing finite affine planes is as follows. Consider a finite field $F = \mathbb{F}_q$, $q = p^e$. A **planar function** on F is a function $f : F \rightarrow F$ such that for every nonzero $d \in F$, the difference function $\Delta_d f : F \rightarrow F$ defined by $(\Delta_d f)(x) := f(x+d) - f(x)$ is a permutation of F .

Proposition 14.1. If $\text{char } F$ is odd, then every quadratic polynomial $f(x) \in F[x]$ represents a planar function on F .

Proof. Let $f(x) = ax^2 + bx + c$ where $a, b, c \in F$ with $a \neq 0$. Then for all nonzero $m \in F$, $\Delta_m f(x) = 2amx + am^2 + b$ is a polynomial of degree 1 (since $2am \neq 0$ in odd characteristic) and hence a permutation of F . \square

The interest in planar functions (and the explanation for their name) derives from the fact that every planar function $f : F \rightarrow F$ gives rise to a finite affine plane \mathcal{A}_f of order q (and hence also a projective plane of the same order). This plane has q^2 points $(x, y) \in F^2$ and $q(q+1)$ lines $\tilde{\ell}_{m,h}$ where $m \in F \cup \{\infty\}$, $h \in F$, defined as follows:

- ‘Vertical’ lines are point sets of the form $\tilde{\ell}_{\infty,k} := \{k\} \times F = \{(k, y) : y \in F\}$ for $k \in F$. Each such line is denoted also by its equation $x = k$.
- ‘Nonvertical’ lines are point sets of the form $\tilde{\ell}_{m,h} := \{(x, f(x+m)+h) : x \in F\}$ where $m, h \in F$. Each such line is denoted also by its equation $y = f(x+m)+h$.

One readily verifies that the resulting structure is an affine plane of order q . For example if $m \neq n$ in F , the fact that $\tilde{\ell}_{m,h} \cap \tilde{\ell}_{n,k}$ contains a unique point (x, y) follows from the fact that $\Delta_{m-n} f(x') = f(x+m) - f(x+n) = k - h$ has a unique solution for $x' := x+n$ in F .

Unfortunately, however, if one uses a quadratic polynomial $f(x) = ax^2 + bx + c \in F[x]$ ($a \neq 0$) as our choice of planar function, the resulting plane is not new; it is just a disguised version of the classical plane. To see this, observe that $(x, y) \in \tilde{\ell}_{m,h}$ iff $y - ax^2 = 2am + a^2m + h$ iff $(x, y - ax^2) \in \ell_{2am, a^2m+h}$. (The description of vertical lines does not change under this recoordination.) The map $(x, y) \mapsto (x, y - ax^2)$ gives an isomorphism from \mathcal{A}_f to the classical plane of order p .

A great deal of effort has been expended on looking for new planar functions, in the search for new nonclassical finite projective planes. Some non-quadratic planar functions [DO] have been known since 1968 (including those constructed in Exercise #1); however the planes constructed from them belong to a large recognized class of planes known as *translation planes*. In 1997, Coulter and Matthews [CM] published a construction of planar functions, which give rise to planes which are not classical, nor are they more general translation planes. Their construction has $q = 3^e$ with $e \geq 4$ (in particular, the order is not prime). The main result of this Section is that for prime order fields, every planar function is quadratic and so the associated plane is classical. This result was obtained independently, and almost simultaneously, by three teams of researchers: Rónyai and Szőnyi [RS], Hiramine [Hi], and Gluck [Gl]. We present here the proof by Gluck because it is arguably the least technical, and because it beautifully demonstrates the natural role played by cyclotomic fields in finite geometry; but also because his approach lends itself naturally to certain generalizations [M3] which we will describe in Section 15.

In the following Theorem 14.2, the equivalence (a) \leftrightarrow (d) appears explicitly in [Gl], [RS] and [Hi]. The equivalence of these statements with (b) and (c), which is easily inferred from Gluck [Gl], will be useful in Section 15.

Theorem 14.2. Let $f : F \rightarrow F$ where $F = \mathbb{F}_p$. Then the following four conditions are equivalent.

- (a) f is a planar function.
- (b) For all $m, m', b, b' \in F$ with $m \neq 0$, the function $\tilde{f} : F \rightarrow F$ defined by $\tilde{f}(x) = f(mx+b) + m'x + b'$ has exponential sum satisfying $|S_{\tilde{f}}| = \sqrt{p}$.
- (c) For all $m \in F$, the function $\tilde{f} : F \rightarrow F$, $\tilde{f}(x) = f(x) + mx$ has exponential sum satisfying $|S_{\tilde{f}}| = \sqrt{p}$.
- (d) f is represented by a quadratic polynomial in $F[x]$; i.e. there exist $a, b, c \in F$ with $a \neq 0$ such that $f(x) = ax^2 + bx + c$ for all $x \in F$.

Proof. The implication (d) \Rightarrow (a) follows from Proposition 14.1; and the implication (b) \Rightarrow (c) is trivial. It remains to prove (a) \Rightarrow (b) and (c) \Rightarrow (d). We start by assuming (a).

Let $f : F \rightarrow F$ be a planar polynomial over $F = \mathbb{F}_p$, p an odd prime. Consider the $p \times p$ matrix $M = [\zeta^{f(x-y)} : x, y \in F]$. Denoting the conjugate-transpose of M by M^* , the (x, y) -entry of MM^* is

$$\sum_{z \in F} \zeta^{f(x-z)} \overline{\zeta^{f(z-y)}} = \sum_{z \in F} \zeta^{f(x-z) - f(y-z)} = \sum_{z \in F} \zeta^{(\Delta_{x-y}f)(y-z)} = \begin{cases} 0, & \text{if } x \neq y; \\ p, & \text{if } x = y \end{cases}$$

by the definition of a planar polynomial. This says that $MM^* = pI$ where I is the $p \times p$ identity matrix; in other words, $\frac{1}{\sqrt{p}}M$ is unitary. In particular, every eigenvalue of M has absolute value equal to \sqrt{p} . Consider the all-ones vector $\mathbf{1}$ of length p . It is easy to see that each entry of $M\mathbf{1}$ equals S_f , the exponential sum of f . So $|S_f| = \sqrt{p}$.

Now given $m, m', b, b' \in F$ with $m \neq 0$, the function

$$\tilde{f} : F \rightarrow F, \quad x \mapsto f(mx+b) + m'x + b'$$

is evidently also planar: for all nonzero $d \in F$, we have

$$\Delta_d \tilde{f} : F \rightarrow F, \quad x \mapsto (\Delta_{md}f)(mx+b) + m'd$$

which is clearly a permutation of F because $\Delta_{md}f$ is a permutation of F . Applying the preceding argument to \tilde{f} in place of f , we obtain (b).

Finally, assume (c). By Cavior's Theorem 13.4, the multiset of values of f coincides with the multiset of values of some quadratic polynomial $g : F \rightarrow F$. In particular, f assumes no value more than twice. The same is true for every function $\tilde{f} : F \rightarrow F$ of the form $\tilde{f}(x) = f(x) + mx$ for $m \in F$. This means that in F^2 , the graph of f intersects any non-vertical line $y = -mx + b$ at most twice. By Segre's Theorem 3.14, f is represented by a quadratic polynomial, so (d) holds; and we have seen that \mathcal{A}_f is isomorphic to the classical plane of order p in this case. \square

The only known planes of prime order are the classical planes constructed from \mathbb{F}_p ; and it is tempting to conjecture that planes of prime order must be classical. (But once again, keep in mind The Streetlight Effect.) Theorem 14.2 is the strongest result known in this direction. The planes \mathcal{A}_f constructed from planar functions f share a special feature in common with the classical planes: Each of these planes admits an elementary abelian group of automorphisms of order p^2 which transitively permutes the points: For each $(r, s) \in F^2$, the translation map $(x, y) \mapsto (x+r, y+s)$ takes $\ell_{\infty, a}$ to $\ell_{\infty, a+s}$, and takes $\ell_{m, b}$ to $\ell_{m-r, b+s}$ for $m \neq \infty$. Prior to Theorem 14.2, it was already known (using a combination of geometric and group-theoretic arguments, which we omit here) that *any* affine plane of prime order p , whose automorphism group has order divisible by p^2 , must be of the form \mathcal{A}_f for some planar polynomial f . Thus Theorem 14.2 yields the important consequence

Corollary 14.3. Any affine plane of prime order p whose automorphism group has order divisible by p^2 , must be classical.

Exercises 14.

1. Let $E = \mathbb{F}_q$, $q = p^e$, p an odd prime. Fix an automorphism $\sigma \in \text{Aut } E$; thus $\sigma(x) = x^{p^k}$ for some $k \in \{0, 1, 2, \dots, e-1\}$. Show that the function $f : E \rightarrow E$, $f(x) = x\sigma(x) = x^{p^k+1}$ is a planar function on F iff $\frac{e}{\gcd(k, e)}$ is odd. (Note that $\sigma \in \text{Aut } E$ has order $\frac{e}{\gcd(k, e)}$.)
2. Consider the quadratic extension $E \supset F$ of fields of order q^2 and q , where q is odd. Recall that $\sigma : E \rightarrow E$, $\sigma(x) = x^q$ is the automorphism of order 2 with fixed field F . Define a new binary operation on E by

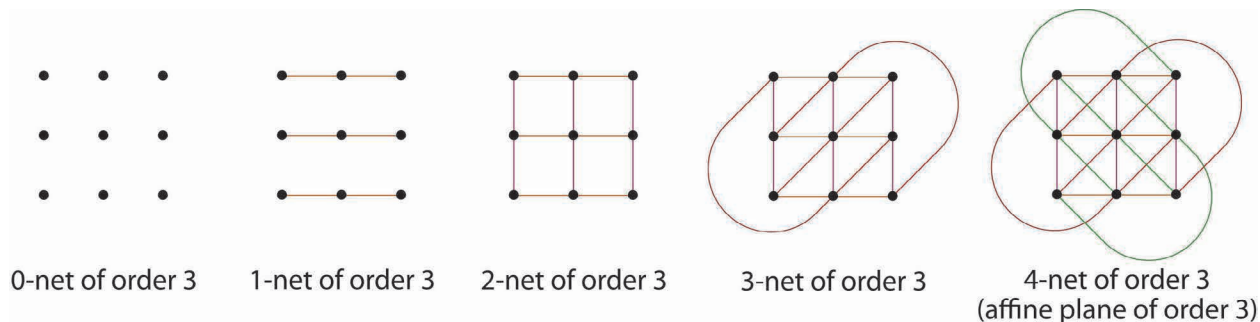
$$x * y = \begin{cases} xy, & \text{if } x \text{ is a square (zero or nonzero square);} \\ x\sigma(y), & \text{if } x \text{ is a nonsquare.} \end{cases}$$
 - (a) Prove that ‘ $*$ ’ is associative and left-distributive, i.e. $(x * y) * z = x * (y * z)$ and $x * (y + z) = x * y + x * z$ for all $x, y, z \in E$.
 - (b) Prove that the nonzero elements of E form a nonabelian group under the operation ‘ $*$ ’.
 - (c) Although ‘ $*$ ’ is not right-distributive, this is compensated for by a weaker property which you should show: if $a, b, c \in E$ with $a \neq b$, then the equation $a * x = b * x + c$ has a unique solution $x \in E$.
 - (d) Show that the following structure is an affine plane of order q^2 , where we essentially replace ordinary multiplication by ‘ $*$ ’. Take points to be ordered pairs $(x, y) \in E^2$. There are two types of lines:
 - q ‘vertical’ lines $x = k$, i.e. point sets $\{(k, y) : y \in E\}$ for $k \in E$; and
 - q^2 ‘nonvertical’ lines $y = m * x + b$, i.e. point sets $\{(x, m * x + b) : x \in F\}$, where $m, b \in E$.
 This construction gives one of the most standard classes of translation planes.

15. Nets

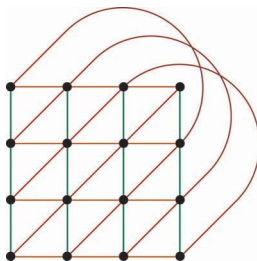
A **k -net of order n** is an incidence system of n^2 points and kn subsets of the points called lines, such that

- each point is on k lines, and each line has n points;
- parallelism is an equivalence relation on the set of lines, where two lines ℓ, ℓ' are **parallel** (denoted $\ell \parallel \ell'$) if they are either equal or disjoint;
- each parallel class of lines (i.e. equivalence class under parallelism) consists of n lines which partition the point set;
- any two distinct lines meet in either 0 or 1 points.

Clearly $k \leq n + 1$ here; and an $(n + 1)$ -net of order n is the same thing as an affine plane of order n . Here are all the nets of order 3, up to isomorphism:



If one hopes to build an affine plane of order n , one might reasonably try to do so incrementally by starting with n^2 points and adding one parallel class at a time, hoping to see how far one might go. The first two parallel classes (which one may take to be ‘horizontal’ and ‘vertical’ lines) are trivially constructed. For every $n \geq 2$ it is possible to find a third parallel class of lines extending this to a 3-net of order n . Now the construction process becomes more delicate. While there exist 3-nets of order 6, none of them are extendible to 4-nets (a fact known already to Euler); and this implies the nonexistence of an affine plane of order 6. Although there exists a 5-net of order 4 (affine plane of order 4), there exist 3-nets of order 4 which *are not extendible* to any 4-net or 5-net of order 4. Here is an example of a maximal 3-net of order 4, i.e. one which cannot be extended to a 4-net:



And although 4-nets of order 10 have been constructed, it is not known whether or not there exists a 5-net of order 10 (although no 11-net of order 10 exists, by Lam et al).

Here we describe an algebraic approach to studying finite nets, which (in our view) is more promising than other approaches that have been tried. To simplify the exposition, we assume here that $n = p$ is prime. Our goal is to show that every plane of prime order p is classical (a major open problem).

To introduce this approach, we first consider the nets of order 3 shown above. Each successive parallel class may be described by a triple of matrices, starting with A_0, A_1, A_2 for the first parallel class; B_0, B_1, B_2 for the second parallel class, etc., where

$$\begin{array}{cccc} A_0 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} & B_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} & C_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} & D_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ A_1 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} & B_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} & C_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} & D_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \\ A_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} & B_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} & C_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} & D_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

Here the p^2 points may be viewed as the pairs (i, j) with $i, j \in F$ where $F = \mathbb{F}_p$; and each matrix has 1's in the positions of a line, with the other entries equal to zero. (The choice of \mathbb{F}_3 as an index set here is purely a matter of convenience. Any set of $p = 3$ symbols could be used in its place.) Note that

$$(15.1) \quad A_0 + A_1 + A_2 = B_0 + B_1 + B_2 = C_0 + C_1 + C_2 = D_0 + D_1 + D_2 = J \text{ where } J = J_3, \text{ the } 3 \times 3 \text{ matrix of 1's.}$$

Denote by \mathcal{C}_k the F -span of the matrices from the first k parallel classes, a k -net of order p . We are interested in the dimensions of the sequence

$$(15.2) \quad 0 = \mathcal{C}_0 \leq \mathcal{C}_1 \leq \mathcal{C}_2 \leq \cdots \leq \mathcal{C}_{p+1}.$$

In the case $p = 3$ shown above, the subspaces in (15.2) have dimensions 0,3,5,6,6. Now it is the differences $\dim \mathcal{C}_k - \dim \mathcal{C}_{k-1}$ which are of interest. In our example, this is the sequence 3,2,1,0. It is not by coincidence that these values form an arithmetic sequence: for every known plane of prime order p , these values always always form a sequence $p, p-1, p-2, \dots, 2, 1, 0$, independently of which order we list the $p+1$ parallel classes. We pose

$$(15.3) \quad \textbf{Conjecture [M1]:} \text{ For any } k\text{-net of prime order } p \text{ and } (k-1)\text{-subnet thereof, with } k \geq 1, \text{ the subspaces } \mathcal{C}_{k-1} \leq \mathcal{C}_k \text{ constructed as above have dimensions satisfying}$$

$$\dim \mathcal{C}_k - \dim \mathcal{C}_{k-1} \geq p - k + 1.$$

The importance of (15.3) is due to

- Theorem 15.4 [M1].** (i) Subnets of classical planes of prime order satisfy Conjecture 15.3 with equality.
(ii) If Conjecture 15.3 holds for a given prime p , then all planes of order p are classical.

It is known (see e.g. [M1]) that $\dim \mathcal{C}_{p+1} = \frac{1}{2}p(p+1)$ for every affine plane of prime order p . Since $p + (p-1) + \cdots + 2 + 1 + 0 = \frac{1}{2}p(p+1)$, the conjectured lower bound (15.3) would require equality in the case of subnets of planes of order p ; so if one's sole interest is in classifying planes of prime order p , then (15.3) could be replaced by the conjecture that for subnets of planes of order p , $\dim \mathcal{C}_k - \dim \mathcal{C}_{k-1} = p - k + 1$. However, there are many nets of prime order where strict inequality holds in (15.3); and it is conceivable that proving the lower bound (15.3) in the more general setting of nets (not necessarily extendible to planes) may be more natural or easier than proving equality. In Theorem 15.7 below, we prove the first nontrivial case of Conjecture 15.3, the case $k = 3$. But first we rephrase the descriptions both of the nets, and of the dimensions of the spaces \mathcal{C}_i .

The p^2 points of a k -net can be taken to be k -tuples $x = (x_1, x_2, \dots, x_k) \in F^k$, $F = \mathbb{F}_p$, where $a_i \in F$ indexes which line of the i th parallel class passes through the point x . Thus in our example above, $x_i = 0, 1$ or 2 according as A_i has entry 1 in the position corresponding to the point x ; and the 4-net is seen to be $\{(x, y, x+y, x-y) : x, y \in F\}$ where $F = \mathbb{F}_3$. In general,

Theorem 15.5. Let F be an arbitrary set of n symbols, and let $k \geq 2$.

- (i) Suppose $\mathcal{N} \subseteq F^k$ is a subset of the k -tuples over F of size $|\mathcal{N}| = n^2$ such that for all $i \neq j$ in $\{1, 2, \dots, k\}$, the projection $\mathcal{N} \rightarrow F^2$, $(x_1, x_2, \dots, x_k) \mapsto (x_i, x_j)$ is surjective. (Thus every vector in \mathcal{N} is uniquely determined by its i th and j th coordinates.) Then \mathcal{N} is the point set of a k -net of order n whose i th parallel class ($i \in \{1, 2, \dots, k\}$) are the subsets $\{x \in \mathcal{N} : x_i = a\}$ for $a \in F$.
- (ii) Every k -net of prime order n is isomorphic to a net of the form described in (i). \square

We omit the proof of Theorem 15.5, which is straightforward. The notion of a k -net of order n appears in many guises in the combinatorial literature (particularly as a set of $k-2$ mutually orthogonal Latin squares of order n , an orthogonal array $OA(k, n)$, a transversal design $TD(k, n)$). See [ACD] for details, noting that our set of n^2 vectors of length k above, when transposed, form the columns of an $OA(k, n)$.

Now consider a k -net \mathcal{N} of order n , $k \geq 3$. We will often write $\mathcal{N} = \mathcal{N}_k$ to emphasize that it is a k -net. We may assume $\mathcal{N}_k \subseteq F^k$ has the form described in Theorem 15.5(i). Deleting the i th coordinate from all vectors in \mathcal{N}_k gives a $(k-1)$ -net of the same order n , which we call a **$(k-1)$ -subnet** of the original net \mathcal{N}_k . A k -net \mathcal{N} has exactly k choices of $(k-1)$ -subnet, each of which is formed by omitting one of the k parallel classes of lines in \mathcal{N} . Note that a 2-net is necessarily $\mathcal{N}_2 = F^2$. The **classical** (or **desarguesian**) affine planes of prime order p , as described in the notation of Theorem 15.5, have the form

$$\{(x, y, x+y, x+2y, \dots, x+(p-1)y) : x, y \in F\}, \quad F = \mathbb{F}_p$$

up to isomorphism. Moreover, any k -net obtained from one of these classical planes by deleting ('puncturing') $p+1-k$ of its coordinates, gives a k -subnet which we *also* call

classical or **desarguesian**. Classical 3-nets can always be reCOORDINATIZED to have the form $\{(x, y, x+y) : x, y \in F\}$; such 3-nets are also called **cyclic**.

Arbitrary k -nets of order p cannot be expected to admit an algebraic description as in the classical case described above, and so \mathbb{F}_p can then be replaced by an arbitrary index set of size p . Yet we will continue to use $F = \mathbb{F}_p$ as our chosen index set in the general case, as a matter of convenience.

Given a k -net \mathcal{N}_k of order p as above, denote by $\mathcal{V} = \mathcal{V}_k$ the vector space over F consisting of all k -tuples of functions (f_1, f_2, \dots, f_k) such that $f_i : F \rightarrow F$ satisfying

$$f_1(x_1) + f_2(x_2) + \dots + f_k(x_k) = 0 \quad \text{for all } (x_1, x_2, \dots, x_k) \in \mathcal{N}_k.$$

In other words, if M is the $kp \times p^2$ incidence matrix of \mathcal{N}_k (with rows indexed by points, and columns indexed by lines) then \mathcal{V}_k is essentially the (right) null space of M over F . By the Fundamental Theorem of Linear Algebra,

$$\dim \mathcal{C}_k + \dim \mathcal{V}_k = kp$$

where \mathcal{C}_k is the column space of M over F . (Although \mathcal{C}_k has the same dimension as the row space of M , the column space is interpreted more naturally—this being the subspace of F^{p^2} spanned by the characteristic vectors of the lines of the net, as in our original example for $p = 3$.) In terms of the spaces \mathcal{V}_k , we may reformulate the conjectured inequality (15.3) as $\dim \mathcal{V}_k - \dim \mathcal{V}_{k-1} \leq k - 1$ for $k \geq 1$.

Now consider the constant function $\mathbb{1} : F \rightarrow F$, $\mathbb{1}(a) = 1$ for all $a \in F$; and observe that $(a_1\mathbb{1}, a_2\mathbb{1}, \dots, a_k\mathbb{1}) \in \mathcal{V}_k$ for all choices of scalars $a_i \in F$ satisfying $a_1 + a_2 + \dots + a_k = 0$. These particular k -tuples of functions form a $(k - 1)$ -dimensional subspace $\mathcal{V}_k^{(0)} \leq \mathcal{V}_k$, and we obtain a splitting

$$\mathcal{V}_k = \mathcal{V}_k^{(0)} \oplus \mathcal{U}_k$$

where \mathcal{U}_k is the subspace consisting of all $(f_1, f_2, \dots, f_k) \in \mathcal{V}_k$ such that $f_1(0) = f_2(0) = \dots = f_k(0) = 0$. This splitting is obtained by noting that the map $\mathcal{V}_k \rightarrow \mathcal{V}_k^{(0)}$, $(f_1, f_2, \dots, f_k) \mapsto (f_1(0)\mathbb{1}, f_2(0)\mathbb{1}, \dots, f_k(0)\mathbb{1})$ is a projection with \mathcal{U}_k as its kernel. This simplifies Conjecture 15.3 further, leading to the equivalent form

(15.6) **Conjecture:** For any k -net of prime order p and $(k - 1)$ -subnet thereof, $k \geq 2$, the subspaces $\mathcal{U}_{k-1} \leq \mathcal{U}_k$ constructed as above have dimensions satisfying

$$\dim \mathcal{U}_k - \dim \mathcal{U}_{k-1} \leq k - 2.$$

As an example, for the 3-net of order 3 presented by the matrices A_i, B_i, C_i , $i = 0, 1, 2$ as above, the one nontrivial relation between the first three parallel classes is

$$A_1 - A_2 + B_1 - B_2 - C_1 + C_2 = 0,$$

giving $(\iota, \iota, -\iota) \in \mathcal{U}_3$ where $\iota(a) = a$ for all $a \in \mathbb{F}_3$; and in this case \mathcal{U}_3 is one-dimensional spanned by $(\iota, \iota, -\iota)$. The first nontrivial case of (15.6) says that for every 3-net of prime order, $\dim \mathcal{U}_3 \leq 1$. This is verified as follows.

Theorem 15.7 ([M1,M3]). Conjectures (15.3) and (15.6) hold for $k = 3$. In fact for any 3-net of prime order p , we have $\dim \mathcal{U}_3 \leq 1$; and equality holds iff the net is cyclic, i.e. isomorphic to $\{(x, y, x+y) : x, y \in \mathbb{F}_p\}$.

Proof. Let $\mathcal{N}_3 \subset F^3$ be a 3-net of order p , $F = \mathbb{F}_p$; and let $\zeta = \zeta_p$. Without loss of generality, there exists a nonzero triple $(f_1, f_2, f_3) \in \mathcal{U}_3$. The exponential sums $S_{f_i} = \sum_{a \in F} \zeta^{f_i(a)}$ satisfy

$$\begin{aligned} S_{f_1} S_{f_2} &= \left(\sum_{a \in F} \zeta^{f_1(a)} \right) \left(\sum_{b \in F} \zeta^{f_2(b)} \right) = \sum_{a, b \in F} \zeta^{f_1(a) + f_2(b)} \\ &= \sum_{(a, b, c) \in \mathcal{N}_3} \zeta^{f_1(a) + f_2(b)} = p \sum_{c \in F} \zeta^{-f_3(c)} = p \overline{S_{f_3}} \end{aligned}$$

since $f_1(a) + f_2(b) + f_3(c) = 0$ for all $(a, b, c) \in \mathcal{N}_3$. Multiplying both sides by S_{f_3} , and then using the same argument for the other pairs of subscripts in $\{1, 2, 3\}$, gives

$$S_{f_1} S_{f_2} S_{f_3} = p |S_{f_1}|^2 = p |S_{f_2}|^2 = p |S_{f_3}|^2.$$

Now if any of the exponential sums S_{f_i} is nonzero, they must all be nonzero and we obtain $|S_{f_1}| = |S_{f_2}| = |S_{f_3}| = p$; but then by Lemma 13.1(i), each of the functions f_i is constant. But since $(f_1, f_2, f_3) \in \mathcal{U}_3$, we have $f_1(0) = f_2(0) = f_3(0) = 0$. This forces $f_1 = f_2 = f_3 = 0$, a contradiction.

Thus $S_{f_1} = S_{f_2} = S_{f_3} = 0$. By Lemma 13.1(ii), each of the functions $f_i : F \rightarrow F$ is a permutation. Without loss of generality, $f_1(x) = f_2(x) = x$ and $f_3(x) = -x$ for all $x \in F$; for if not, then we simply relabel the p lines in each of the three parallel classes such that this is the case. Now every $(a, b, c) \in \mathcal{N}_3$ satisfies

$$c = -f_3(c) = f_1(a) + f_2(b) = a + b;$$

that is, $\mathcal{N}_3 = \{(a, b, a+b) : a, b \in F\}$. It remains only to verify that for this particular 3-net, every $(g_1, g_2, g_3) \in \mathcal{U}_3$ is a scalar multiple of (f_1, f_2, f_3) . For this, we may assume $g_1(1) = 0$; otherwise replace (g_1, g_2, g_3) by $(g_1, g_2, g_3) - g_1(1)(f_1, f_2, f_3)$. But we now have $g_1(0) = g_1(1) = 0$, so g_1 is no longer a permutation of F , and the argument above then forces $g_1 = g_2 = g_3 = 0$ as required. \square

At this time we do not have a proof of Conjecture (15.3) or (15.6) for $k = 4$; but we have some partial results. Our analysis of 4-nets begins with the following extension of Theorem 15.7.

Lemma 15.8 ([M3]). Let \mathcal{N}_4 be a 4-net of prime order p , and let $(f_1, f_2, f_3, f_4) \in \mathcal{U}_4$. Then either

- (i) three or more of f_1, f_2, f_3, f_4 are permutations, or
- (ii) $|S_{f_1}| = |S_{f_2}| = |S_{f_3}| = |S_{f_4}| > 0$.

Proof. As usual, let $\zeta = \zeta_p$. For all $(x_1, x_2, x_3, x_4) \in \mathcal{N}_4$ we have $f_1(x_1) + f_2(x_2) + f_3(x_3) + f_4(x_4) = 0$, so $\zeta^{f_1(x_1)+f_2(x_2)} = \zeta^{-f_3(x_3)-f_4(x_4)}$. Summing over all $(x_1, x_2, x_3, x_4) \in \mathcal{N}_4$ gives

$$S_{f_1} S_{f_2} = \overline{S_{f_3} S_{f_4}}.$$

Multiplying both sides by $\overline{S_{f_2}}$ gives

$$S_{f_1} |S_{f_2}|^2 = \overline{S_{f_2} S_{f_3} S_{f_4}}.$$

By symmetry, we must have in fact

$$S_{f_1} |S_{f_2}|^2 = S_{f_1} |S_{f_3}|^2 = S_{f_1} |S_{f_4}|^2 = \overline{S_{f_2} S_{f_3} S_{f_4}}$$

and

$$S_{f_1} (|S_{f_2}|^2 - |S_{f_3}|^2) = S_{f_1} (|S_{f_2}|^2 - |S_{f_3}|^2) = 0.$$

Now we may suppose at least one of the exponential sums S_{f_i} is nonzero, otherwise case (i) holds. So without loss of generality, $S_{f_1} \neq 0$. Then we directly obtain $|S_{f_2}| = |S_{f_3}| = |S_{f_4}|$. If the latter three exponential sums vanish, we obtain case (i); otherwise by symmetry we obtain case (ii). \square

In the following, we write $(0, x, x, x) \in \mathcal{U}_4$ as an abbreviation for $(0, \iota, \iota, \iota) \in \mathcal{U}_4$ where $\iota(x) = x$ for $x \in F$.

Lemma 15.9 ([M3]). Suppose that \mathcal{N}_4 is a 4-net of prime order p for which there exist linearly independent 4-tuples $(f_1, f_2, f_3, f_4), (0, x, x, x) \in \mathcal{U}_4$. Then either

- (i) $|S_{f_1}| = |S_{f_2}| = |S_{f_3}| = |S_{f_4}| = \sqrt{p}$ and f_2, f_3, f_4 are quadratic polynomials; or
- (ii) $S_{f_1} = 0$ and at least two of f_2, f_3, f_4 are scalar multiples of $\iota, \iota(x) = x$.

Proof. Suppose first that $S_{f_1} \neq 0$. For all $a \in F$, $(f_1, f_2, f_3, f_4) + a(0, x, x, x) \in \mathcal{U}_4$; so Lemma 15.8 gives either

$$S_{f_2(x)+ax} = S_{f_3(x)+ax} = S_{f_4(x)+ax} = 0$$

or

$$|S_{f_2(x)+ax}| = |S_{f_3(x)+ax}| = |S_{f_4(x)+ax}| = |S_f| > 0.$$

By Theorem 13.5, and using the fact that $f_2(0) = f_3(0) = f_4(0) = 0$, we obtain either conclusion (i) or $f_2 = f_3 = f_4 = a\iota$ for some $a \in F$; but in the latter case, we get $(f_1, 0, 0, 0) = (f_1, f_2, f_3, f_4) - a(0, \iota, \iota, \iota) \in \mathcal{U}_4$, forcing $f_1 = 0$, a contradiction.

Hence we may assume that $S_{f_1} = 0$, so f_1 is a permutation. Without loss of generality $f_1 = \iota$ (otherwise relabel lines in the first parallel class so that this is the case). By Lemma 15.8, the three sets $A_{f_2}, A_{f_3}, A_{f_4}$ (see Lemma 13.6) are mutually disjoint. Without loss of generality, $|A_{f_2}| \leq |A_{f_3}| \leq |A_{f_4}|$; otherwise permute the last three parallel classes such that this inequality holds. Thus $|A_{f_2}| \leq |A_{f_3}| \leq \frac{1}{3}p \leq \frac{1}{2}(p-1)$. By Lemma 13.6 and the condition $f_2(0) = f_3(0) = 0$, we have $f_2 = a\iota$ and $f_3 = b\iota$ for some $a, b \in F$, so conclusion (ii) holds. \square

Recall that a 4-net \mathcal{N}_4 has four 3-subnets, each formed by deleting one of the four parallel classes of lines from \mathcal{N}_4 (or equivalently, by puncturing one of the four coordinates).

Theorem 15.10 ([M3]). Let \mathcal{N}_4 be a 4-net of prime order p . Then the number of its cyclic 3-subnets is always 0, 1, 3 or 4, but never exactly 2.

Proof. We must show that if \mathcal{N}_4 has at least two cyclic 3-subnets, then it has a third. Without loss of generality, parallel classes 1,2,3 of \mathcal{N}_4 form a cyclic 3-subnet; and so do parallel classes 2,3,4. After relabelling lines in each parallel class, we have $(f_1, f_2, f_3, 0), (0, x, x, x) \in \mathcal{U}_4$ where f_1, f_2, f_3 are permutations of F . By Lemma 15.9, we may suppose that $f_2(x) = ax$ for some $a \in F$. Now

$$(f_1(x), 0, f_3(x) - ax, -ax) = (f_1, f_2, f_3, 0) - a(0, x, x, x) \in \mathcal{U}_4$$

so that \mathcal{N}_4 has a third cyclic 3-subnet on parallel classes 1,3,4. \square

Remark: Theorem 15.10 is best possible in the sense that there exist 4-nets of prime order for which the number of cyclic 3-subnets is 0, 1, 3 or 4.

Recall that a classical 4-net of order p is one of the form $\{(x, y, x+y, x+cy) : x, y \in F\}$ for some $c \in F$ with $c \neq 0, 1$. For choices of $p > 5$, there are generally many nonisomorphic 4-nets of order p ; different choices of c sometimes yield isomorphic 4-nets, but usually not.

Theorem 15.11 ([M3]). Let \mathcal{N}_4 be a 4-net of prime order p . Then \mathcal{N}_4 is classical (i.e. desarguesian) iff all four of its 3-subnets are cyclic.

Proof. As in the proof of Theorem 15.10, we may suppose that

$$(f_1, f_2, f_3, 0), (0, x, x, x), (f_1, 0, f_3 - ax, -ax) \in \mathcal{U}_4$$

for some fixed (and evidently nonzero) $a \in F$; and each of the nine nonzero coordinates appearing in these 4-tuples is a permutation of F . Without loss of generality (again, by permuting the labels on the lines of the first parallel class of lines) we have $f_1(x) = x$. By hypothesis, there also exist permutations g_1, g_2, g_4 of F such that

$$(g_1, g_2, 0, g_4) \in \mathcal{U}_4.$$

By Lemma 15.9, either $g_2(x) = bx$ or $g_4(x) = bx$ for some $b \in F$. We may assume that $g_2(x) = bx$; otherwise interchange the second and fourth parallel classes (replacing also a by $-a$, and $f_3(x)$ by $f_3(x) - ax$). Now

$$(g_1(x), 0, -bx, g_4(x) - bx) = (g_1, g_2, 0, g_4) - b(0, x, x, x) \in \mathcal{U}_4$$

so by Theorem 15.7, this is a scalar multiple of $(x, 0, f_3(x) - ax, -ax)$. Without loss of generality (after applying a suitable scalar multiple),

$$(g_1(x), 0, -bx, g_4(x) - bx) = (x, 0, f_3(x) - ax, -ax).$$

This forces

$$\mathcal{N}_4 = \{(bx + ay, -x - y, x, y) : x, y \in F\}. \quad \square$$

Theorem 15.12 ([M3]). Let \mathcal{N}_4 be a 4-net of prime order p , and suppose that \mathcal{N}_4 has a cyclic 3-subnet \mathcal{N}_3 . Then Conjectures 15.3 and 15.6 hold for \mathcal{N}_4 . Indeed, $\dim \mathcal{U}_4 \leq 3$; and equality holds iff \mathcal{N}_4 is isomorphic to a 4-subnet of a classical plane of order p .

Proof. We may suppose that $\dim \mathcal{U}_4 \geq 3$ and that

$$(f_1, f_2, f_3, f_4), (g_1, g_2, g_3, g_4), (0, x, x, x) \in \mathcal{U}_4$$

are linearly independent. By Theorem 15.7, the functions f_1 and g_1 are nonzero. More than this, f_1 and g_1 are linearly independent functions $F \rightarrow F$; for if $f_1 = ag_1$ for some $a \in F$, then

$$(f_1, f_2, f_3, f_4) - a(g_1, g_2, g_3, g_4) = b(0, x, x, x)$$

for some $b \in F$, a contradiction.

By Lemma 15.9 we have $|S_{f_1}| \in \{0, \sqrt{p}\}$. More generally, for all $a, b \in F$ the function $f = af_1 + bg_1$ satisfies $|S_f| \in \{0, \sqrt{p}, p\}$; so by Theorem 13.11, $f_i(x) = a_i^2 \sigma(x)^2 + b_i \sigma(x)$ for some $a_i, b_i \in F$ and some permutation $\sigma : F \rightarrow F$. We may assume $\sigma(x) = x$, after relabelling lines in the first parallel class; and $f_1(x) = x$, $g_1(x) = x^2$, after a change of basis for \mathcal{U}_4 . By Lemma 15.9, we may assume that

$$(x, a_2x, a_3x, f_4(x)), (x^2, g_2(x), g_3(x), g_4(x)), (0, x, x, x) \in \mathcal{U}_4$$

where $a_2, a_3 \in F$ and g_2, g_3, g_4 are quadratic. In particular, we have nonzero tuples

$$(x, 0, (a_3 - a_2)x, f_4(x) - a_2x), (x, (a_2 - a_3)x, 0, f_4(x) - a_3x) \in \mathcal{U}_4$$

and so the 3-subnet formed by parallel classes 1,3,4 is cyclic; likewise the 3-subnet formed by parallel classes 1,2,4. Since

$$(x^2, g_2(x), g_3(x), g_4(x)) + (x, a_2x, a_3x, f_4(x)) \in \mathcal{U}_4,$$

$f_4 + g_4$ is quadratic by Lemma 15.9; and since g_4 is itself quadratic, this forces f_4 to be polynomial of degree ≤ 2 . This means that $f_4(x) = ag_4(x) + bx$ for some $a, b \in F$; and so

$$(ax^2 - x, ag_2(x) + (b - a_2)x, ag_3(x) + (b - a_3)x, 0) \in \mathcal{U}_4.$$

This means that the 3-subnet formed by parallel classes 1,2,3 is cyclic (and $a = 0$). The result follows by Theorem 15.11. \square

Exercises 15.

1. We have illustrated a cyclic 3-net of order 4. Prove that it is maximal; i.e. it is not a subnet of any 4-net of order 4.
2. Let \mathcal{N} be a k -net of prime order p , $2 \leq k \leq p$, in the standard form given by Theorem 15.5(i). Consider a k -tuple of functions (f_1, f_2, \dots, f_k) , $f_i : F \rightarrow F$, such that $f_1(x_1) + f_2(x_2) + \dots + f_k(x_k) = 0$ for all $(x_1, x_2, \dots, x_k) \in \mathcal{N}$; thus $(f_1, f_2, \dots, f_k) \in \mathcal{V}_k$ as we have defined the space \mathcal{V}_k . Denote $\Sigma_i = \sum_{a \in F} f_i(a)$ for $i = 1, 2, \dots, k$.
 - (a) Fix $a \in F$. By considering all p points $(x_1, x_2, \dots, x_k) \in \mathcal{N}$ with last coordinate $x_k = a$, show that $\Sigma_1 + \Sigma_2 + \dots + \Sigma_{k-1} = 0$.
 - (b) By varying the choice of coordinate, obtain relations similar to that in (a) showing that any $k-1$ of $\Sigma_1, \Sigma_2, \dots, \Sigma_k$ have sum equal to zero.
 - (c) Show that $\Sigma_1 = \Sigma_2 = \dots = \Sigma_k = 0$.
 - (d) Let $\varepsilon = 1 - \zeta$ where $\zeta = \zeta_p$. Show that for all $i = 1, 2, \dots, k$, the exponential sum S_{f_i} lies in the ideal $(\varepsilon) \subseteq \mathbb{Z}[\zeta]$.

16. Mutually Unbiased Bases

A **complex Hadamard matrix of order n** is an $n \times n$ matrix H with complex entries such that $HH^* = nI_n$ where H^* is the conjugate transpose of H . Every ordinary Hadamard matrix is a complex Hadamard matrix, but not conversely. Unlike the situation for ordinary Hadamard matrices, complex Hadamard matrices exist for every positive integer n :

Theorem 16.1. Let G be an abelian group of order n . Consider the $n \times n$ matrix H with rows indexed by characters $\chi \in \widehat{G}$ and columns indexed by group elements $g \in G$; and having (χ, g) -entry $\chi(g)$. Then H is a complex Hadamard matrix of order n .

Proof. Orthogonality of the rows of H (with respect to the standard inner product on \mathbb{C}^n) follows from Theorem 6.3(a). \square

The examples constructed in Theorem 16.1 are the **character tables** of the finite abelian groups. For larger values of n , there are typically many other examples than these.

Example 16.2: Some smaller complex Hadamard matrices.

$$\begin{array}{c} \text{Order 2} \\ H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \end{array} \quad
 \begin{array}{c} \text{Order 3} \\ H_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{bmatrix} \end{array} \quad
 \begin{array}{c} \text{Order 4} \\ H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \alpha & -\alpha \\ 1 & -1 & -\alpha & \alpha \end{bmatrix} \end{array} \quad
 \begin{array}{c} \text{Order 6} \\ H_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 \\ 1 & \zeta^2 & \zeta^4 & 1 & \zeta^2 & \zeta^4 \\ 1 & \zeta^3 & 1 & \zeta^3 & 1 & \zeta^3 \\ 1 & \zeta^4 & \zeta^2 & 1 & \zeta^4 & \zeta^2 \\ 1 & \zeta^5 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{bmatrix}; \quad
 H'_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega^2 & \omega^2 & \omega \\ 1 & \omega & 1 & \omega & \omega^2 & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & \omega & 1 \end{bmatrix}
 \end{array}$$

Here we denote $\zeta = \zeta_6$, $\omega = \zeta_3 = \zeta^2$; and α is an arbitrary complex number satisfying $|\alpha| = 1$. For every positive integer n , we may take $\zeta = \zeta_n$ and $H = [\zeta^{xy} : x, y \in \mathbb{Z}/n\mathbb{Z}]$; this gives the character table of the cyclic group of order n . The examples H_2, H_3, H_6 above all arise in this way. When n is not squarefree (i.e. not a product of distinct primes), then there exist noncyclic groups of order n , hence additional character tables arising from Theorem 16.1. For $n = 4$ there are two groups: the cyclic group of order 4 and the Klein 4-group. The choices $\alpha = 1$ or i , in the general form H_4 above, give complex Hadamard matrices equivalent to the character tables of these two groups. ‘Equivalence’ here is under row and column permutations, and scaling individual rows and columns by complex numbers of modulus 1; these operations clearly take complex Hadamard matrices to (equivalent) complex Hadamard matrices. Every complex Hadamard matrix of order 2 or 3 is equivalent to H_2 or H_3 respectively; but for order 4, there are uncountably many equivalence classes of complex Hadamard matrices, due to the continuum of choices for $\alpha \in \mathbb{C}$, $|\alpha| = 1$. (Note that α is not required to be a root of unity, or even algebraic.) Classifying complex Hadamard matrices of order n up to equivalence is a very difficult computational problem; for example it is only rather recently that the case $n = 5$ was settled [Hp], with the result that all are equivalent to the example arising from the cyclic group of order 5. For larger n , there are typically several isolated equivalence classes of complex Hadamard matrices, and several non-isolated classes similar to H_4 .

We will consider \mathbb{C}^n as the set of row vectors of length n over \mathbb{C} ; thus for $u, v \in \mathbb{C}^n$, the standard inner product of u and v may be written as $uv^* \in \mathbb{C}$. A vector $u \in \mathbb{C}^n$ is **flat** if all its entries have modulus $\frac{1}{\sqrt{n}}$. Similarly, an $n \times n$ matrix A is **flat** if all its entries have modulus $\frac{1}{\sqrt{n}}$. Note that for any $n \times n$ complex matrix A , the **Gram matrix** of the rows of A is the matrix AA^* ; its (i, j) -entry is the inner product of rows i and j of A .

Theorem 16.3. Let H be an $n \times n$ complex matrix. The following three conditions are equivalent.

- (i) H is complex Hadamard.
- (ii) $\frac{1}{\sqrt{n}}H$ is a flat unitary matrix.
- (iii) The rows of $\frac{1}{\sqrt{n}}H$ are flat vectors forming an orthonormal basis of \mathbb{C}^n . \square

We omit the proof of Theorem 16.3, which is straightforward. Note that the orthonormal condition of (iii) is with respect to the standard complex inner product: it says that the rows u_1, u_2, \dots, u_n of $\frac{1}{\sqrt{n}}H$ satisfy

$$u_i u_j^* = \delta_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}$$

Let $\mathcal{B} = \{u_1, u_2, \dots, u_n\}, \mathcal{B}' = \{v_1, v_2, \dots, v_n\}$ be two orthonormal bases of \mathbb{C}^n . We say \mathcal{B} and \mathcal{B}' are **unbiased** if $|u_i v_j^*| = \frac{1}{\sqrt{n}}$ for all $i, j \in \{1, 2, \dots, n\}$; equivalently, the matrix of inner products $[u_i v_j^* : i, j \in \{1, 2, \dots, n\}]$ is flat.

The reason why the value $\frac{1}{\sqrt{n}}$ arises throughout, is that it is the only feasible value for $|u_i v_j^*|$, assuming this value is constant. To see this, suppose that c is a positive real constant such that $|u_i v_j^*| = c$ for all i, j . We may expand u_i with respect to the second basis as

$$u_i = c_{i,1}v_1 + c_{i,2}v_2 + \dots + c_{i,n}v_n$$

where $c_{i,j} = u_i v_j^*$ and $|c_{i,j}| = c$. Again using orthonormality, we have

$$1 = \|u_i\|^2 = |c_{i,1}|^2 + |c_{i,2}|^2 + \dots + |c_{i,n}|^2 = nc^2,$$

so $c = \frac{1}{\sqrt{n}}$. The unbiased property for two orthonormal bases is a symmetric (but neither reflexive nor transitive) relation. For a given pair of orthonormal bases, it says that all the vectors of one basis have a fixed ‘angle’ (actually, inner product) with respect to the vectors in the other basis.

Every orthonormal basis is represented by a unitary matrix B having the vectors of \mathcal{B} as its rows. (While the columns of B are also orthonormal, it is only the rows that we consider here.) So it is reasonable to say that two unitary matrices B_1, B_2 are **unbiased** if their rows form an unbiased pair of bases; equivalently, the matrix $B_1 B_2^*$ is flat. Since $B_1 B_2^*$ is also unitary, the latter condition is also equivalent to the condition that $\sqrt{n} B_1 B_2^*$ is complex Hadamard.

Turning this around, every complex Hadamard matrix H of order n gives rise to an unbiased pair of unitary matrices $I_n, \frac{1}{\sqrt{n}}H$ and an unbiased pair of orthonormal bases (the standard basis, forming the rows of I_n ; and the rows of $\frac{1}{\sqrt{n}}H$).

Now consider a set of k orthonormal bases of \mathbb{C}^n , say $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_k$. These bases are **mutually unbiased (of order n)** if \mathcal{B}_i and \mathcal{B}_j are unbiased for all $i \neq j$ in $\{1, 2, \dots, k\}$. Equivalently, a list of unitary $n \times n$ matrices B_1, B_2, \dots, B_k is **mutually unbiased** if $\sqrt{n} B_i B_j^*$ is complex Hadamard for all $i \neq j$ in $\{1, 2, \dots, k\}$.

Example 16.4: Three mutually unbiased bases in \mathbb{C}^2 . The unitary matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

are mutually unbiased where $i = \sqrt{-1}$. Three is the maximum possible number of mutually unbiased bases of order 2.

Example 16.5: Four mutually unbiased bases in \mathbb{C}^3 . The unitary matrices

$$B_\infty = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B_0 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \quad B_1 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & \omega & \omega^2 \\ 1 & \omega^2 & 1 \\ 1 & 1 & \omega^2 \end{bmatrix}, \quad B_2 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & \omega^2 & \omega^2 \\ 1 & 1 & \omega \\ 1 & \omega & 1 \end{bmatrix}$$

are mutually unbiased where $\omega = \zeta_3$. Four is the maximum possible number of mutually unbiased bases of order 3.

Expanding on comments (in Example 16.2) about equivalence of complex Hadamard matrices, let us clarify what it means for two sets of **MUBs** (mutually unbiased bases) to be equivalent. Two sets of MUBs are **equivalent** if one can be obtained from the other by a combination of

- permuting the bases, or permuting the vectors within each basis;
- scaling the individual basis vectors by complex numbers of modulus 1, thus preserving the orthonormal property of each basis; and
- applying a unitary transformation to \mathbb{C}^n (which will simultaneously transform all of the bases to new orthonormal bases which will still be unbiased).

Restated in terms of unitary matrices, this says that if $\{B_1, B_2, \dots, B_k\}$ is a set of k mutually unbiased unitary matrices of order n , then an **equivalent** set is $\{M_1 B_1 U, M_2 B_2 U, \dots, M_k B_k U\}$ where U is an arbitrary unitary $n \times n$ matrix; and M_1, M_2, \dots, M_k are arbitrary **unitary monomial** $n \times n$ matrices. This means that each M_i has a single nonzero entry in each row and each column; and these nonzero entries are complex numbers of modulus 1. Note that since we refer to sets of matrices, their order is not important; this takes care of equivalences due to permutations of the bases.

Quantum logical circuits make extensive use of complex Hadamard matrices as gates; and sets of mutually unbiased bases have applications in quantum information theory, for example in protocols for quantum cryptographic key exchange. While the details of these applications are quite worthy of investigation, we must skip them for lack of available time.

We naturally ask: for each n , how large a set of mutually unbiased bases can be found? How are they constructed in general? These are difficult questions! but some partial answers are known:

Theorem 16.6. Suppose there exists a set of k mutually unbiased bases in \mathbb{C}^n . Then $k \leq n + 1$.

Proof. Denote by V_n the real vector space of all $n \times n$ Hermitian matrices, i.e. V_n is the set of all $A \in \mathbb{C}^{n \times n}$ such that $A^* = A$. Note that $\dim V_n = n^2$; and the standard inner product on V_n is the real inner product defined by $[A, B] = \operatorname{tr}(AB)$ for $A, B \in V_n$. (Note that since $A, B \in V_n$, $\operatorname{tr}(AB) = \operatorname{tr}(\overline{A} \overline{B}) = \operatorname{tr}(A^T B^T) = \operatorname{tr}((BA)^T) = \operatorname{tr}(BA) = \operatorname{tr}(AB)$; so this form is real-valued. Also $\operatorname{tr}(AA) = \operatorname{tr}(AA^*) = \sum_{i,j} |a_{i,j}|^2$ where $A = (a_{i,j})$, so the form is positive definite.)

Suppose $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_k$ are mutually unbiased bases of order n . Write $\mathcal{B}_1 = \{u_1, u_2, \dots, u_n\}$, $\mathcal{B}_2 = \{u_{n+1}, u_{n+2}, \dots, u_{2n}\}$, \dots , $\mathcal{B}_k = \{u_{(k-1)n+1}, u_{(k-1)n+2}, \dots, u_{kn}\}$ and consider the matrices $A_i = u_i^* u_i \in V_n$ for $i = 1, 2, \dots, kn$. We compute $[A_i, A_j]$ in each of three essential cases, noting that $[A_i, A_j] = \text{tr}(A_i A_j) = \text{tr}(u_i^* u_i u_j^* u_j) = \text{tr}(u_i u_j^* u_j u_i^*) = (u_i u_j^*) \overline{(u_i u_j^*)} = |u_i u_j^*|^2$.

For all i , $[A_i, A_i] = |u_i u_i^*|^2 = 1$. If $i \neq j$ but u_i and u_j belong to the same orthonormal basis \mathcal{B}_r , $[A_i, A_j] = |u_i u_j^*|^2 = 0$. Finally, if $u_i \in \mathcal{B}_r$ but $u_j \in \mathcal{B}_s$ with $r \neq s$, we have $[A_i, A_j] = |u_i u_j^*|^2 = \frac{1}{n}$. Thus the Gram matrix of A_1, A_2, \dots, A_{kn} is

$$M = \begin{bmatrix} I_n & \frac{1}{n} J_n & \cdots & \frac{1}{n} J_n \\ \frac{1}{n} J_n & I_n & \cdots & \frac{1}{n} J_n \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n} J_n & \frac{1}{n} J_n & \cdots & I_n \end{bmatrix}.$$

We exhibit the eigenspaces of M acting on \mathbb{C}^{kn} , with each eigenvector partitioned as $[w_1, w_2, \dots, w_k] \in \mathbb{C}^{kn}$ where $w_i \in \mathbb{C}^n$:

- $[\mathbf{1}, \mathbf{1}, \dots, \mathbf{1}]$ is an eigenvector with eigenvalue k , where $\mathbf{1} \in \mathbb{C}^n$ is the vector of 1's;
- there is a $(k-1)$ -dimensional eigenspace for eigenvalue 0, consisting of all $[a_1 \mathbf{1}, a_2 \mathbf{1}, \dots, a_k \mathbf{1}] \in \mathbb{C}^{kn}$ where $a_1, a_2, \dots, a_k \in \mathbb{C}$ satisfying $a_1 + a_2 + \dots + a_k = 0$; and
- there is a $(kn-k)$ -dimensional eigenspace for eigenvalue 1 consisting of all $[w_1, w_2, \dots, w_k] \in \mathbb{C}^{kn}$ where the vectors $w_i \in \mathbb{C}^n$ satisfy $\mathbf{1} w_i^* = 0$.

Since this gives a decomposition of \mathbb{C}^{kn} as a full set of eigenspaces for M , M has rank equal to $kn - k + 1$. But this rank cannot exceed n^2 , since M is the Gram matrix of a set of vectors in the n^2 -dimensional vector space V_n . From $kn - k + 1 \leq n^2$ we obtain $(n-1)k \leq n^2 - 1$ and $k \leq n + 1$. \square

A **complete set of MUBs (mutually unbiased bases) of order n** is a set of $n+1$ MUBs of order n , thus attaining the upper bound of Theorem 16.6. Complete sets of MUBs are known only for prime power values of n ; the question of existence for non-prime-power values of n is an open question. Thus the situation is very much like that for k -nets of order n , where again $k \leq n+1$ and the only known cases where equality holds (giving rise to affine and projective planes of order n) are for prime power values of n . The extent of the relationship between nets and MUBs remains rather mysterious at this time—evidently there are connections; but there does not seem to be any theorem waiting to be discovered, to the effect that if one or the other (affine plane of order n , or complete set of MUBs of order n) exists, so does the other. (Some of the more naive researchers have been drawn down that rabbit hole.) What can be said with assurance, however, is that the most classical constructions of finite affine planes and complete sets of MUBs have several common features. Both use finite fields (which necessarily have prime power order). We prove the following only for q odd; the analogue for q even uses Galois rings

of characteristic 4, which we omit. The infinite family of classical examples to which we refer here, generalizes Examples 16.4 and 16.5.

Theorem 16.7. Let $q = p^e$, p an odd prime. Then there exists a complete set of MUBs of order q .

Proof. Let $B_\infty = I_q$. For each $r \in F = \mathbb{F}_q$, define the $q \times q$ matrix $B_r = \frac{1}{\sqrt{q}} [\zeta^{\text{Tr}(ry^2+xy)} : x, y \in F]$ where $\text{Tr} = \text{Tr}_{F/K}$, $K = \mathbb{F}_p$, $\zeta = \zeta_p$. For all r, s in F , the (x, y) -entry of $B_r B_s^*$ is $\frac{1}{q} S_f$ where $f(z) = (r-s)z^2 + (x-y)z$. When $r \neq s$, $f(z)$ is a quadratic polynomial; so by Theorem 13.3, $|S_f| = \sqrt{q}$ and the matrix $B_r B_s^*$ is flat. When $r = s$, $f(z) = (x-y)z$ and $S_f = 0$ for $x \neq y$; $S_f = q$ for $x = y$ so $B_r B_r^* = I_q$; thus B_r is unitary. Of course, $B_\infty = I_q$ is unitary. Finally, for each $r \in F$, $B_r B_\infty^* = B_r$ is clearly flat. \square

Haagerup [Hp] has showed that every complex Hadamard matrix is equivalent to the construction of Theorem 16.1. We [MM] have extended this result to show that every set of mutually unbiased bases of order 5 is contained (up to equivalence) in the complete set constructed in Theorem 16.7. This result uses our Theorems 13.5 and 13.12, thus lending credence to the belief in a connection between nets and MUBs. However our result relies on Haagerup's uniqueness result [Hp] for the complex Hadamard matrix of order 5. The basic argument works for 2, 3 and 5 where there is a single complex Hadamard matrix up to equivalence, but not for other orders.

Theorem 16.8 ([MM]). Every set of k mutually unbiased bases of order 5 is contained (up to equivalence) in the complete set constructed in Theorem 16.7.

Proof. Throughout our proof we denote

- $F = \mathbb{F}_5$ and $\zeta = \zeta_5$;
- $\mathbb{U}_5 = U_5(\mathbb{C})$, the group of 5×5 unitary matrices over \mathbb{C} ;
- \mathbb{M}_5 is the group of 5×5 unitary monomial matrices. This is the set of matrices of the form $[\lambda_x \delta_{x, \sigma(y)} : x, y \in F]$, $F = \mathbb{F}_5$ where $\lambda_x \in \mathbb{C}$, $|\lambda_x| = 1$, and σ is one of the 120 permutations of F . Every $M \in \mathbb{M}_5$ factors uniquely as $M = PD$ where P is a 5×5 permutation matrix and D is a 5×5 diagonal matrix with complex entries having modulus 1 on its main diagonal;
- $B_r = \frac{1}{\sqrt{5}} [\zeta^{ry^2+xy} : x, y \in F]$ for $r \in F$. These matrices, together with I_5 , form the standard complete set of MUB's from Theorem 16.7. We also denote $B = B_0 = \frac{1}{\sqrt{5}} [\zeta^{xy} : x, y \in F]$ so that $B_r = B[\zeta^{ry^2} \delta_{x,y} : x, y \in F]$ for all $r \in F$.

Haagerup [Hp, Theorem 2.2] has classified the complex Hadamard matrices of order 5:

$$(16.9) \quad \text{Every complex Hadamard matrix of order 5 has the form } MBM' \text{ for some } M, M' \in \mathbb{M}_5.$$

Let us call a complex Hadamard matrix **normalized** if its first row and column consist of 1's. Every complex Hadamard matrix is equivalent to one which is normalized; simply scale each row and column by an appropriate complex number of modulus 1 to obtain such a normalized representative of its equivalence class. Or, we may choose to first permute rows and columns before scaling, thereby obtaining a possibly different normalized matrix in the equivalence class; so the normalized form is not unique in its equivalence class. In particular there is only one equivalence class of complex Hadamard matrices of order 5, but many normalized representatives in this class; see Exercise #2. We prove the following refinement of (16.9):

(16.10) Every complex Hadamard matrix of order 5 has the form MBM' for some $M, M' \in \mathbb{M}_5$ such that M' has entry 1 in its upper left corner.

(It is customary to refer to the upper left corner of a matrix as its $(1, 1)$ -entry; although when we index the entries using elements of \mathbb{F}_5 , it would make more sense to call this the $(0, 0)$ -entry.) Given a complex Hadamard matrix H of order 5, first write it in the form $H = MBM'$ for some $M, M' \in \mathbb{M}_5$ by (16.9). However the leftmost column of this M' has its nonzero entry in the $(i, 0)$ position. It is straightforward to check that the circulant matrix $C = [\delta_{x, y+1} : x, y \in F]$ satisfies $BC = DB$ where $D \in \mathbb{M}_5$ is the diagonal matrix $D = [\zeta^x \delta_{x, y} : x, y \in F]$. The monomial matrix $M'' = C^{-i}M'$ has a nonzero entry (call it λ) in its top left corner, and $H = MBM' = MBC^iM'' = MD^iBM'' = M''BM''$ where $M'', M''' \in \mathbb{M}_5$. Without loss of generality, $\lambda = 1$; otherwise replace M'', M''' by $\bar{\lambda}M'', \lambda M'''$ respectively. This gives the form claimed in (16.10).

(16.11) Every normalized complex Hadamard matrix H of order 5 has fifth roots of unity as entries. The product of the entries in each of its rows is 1; and the same holds for columns.

To verify (16.11), let $H = MBM'$ be a normalized complex Hadamard matrix of order 5, where M, M' are as in (16.10). Comparing leftmost columns on both sides, we see that M must also have entry 1 in its top left corner. Factor $M = DP$ and $M' = P'D'$ where P and P' are permutation matrices (each having 1 in the upper left corner); also $D = \text{diag}(1, \lambda_1, \lambda_2, \lambda_3, \lambda_4)$ and $D' = \text{diag}(1, \lambda'_1, \lambda'_2, \lambda'_3, \lambda'_4)$ are diagonal matrices with $|\lambda_i| = |\lambda'_i| = 1$. Now $H = D(PBP')D'$ where both H and PBP' have 1's in their top row and leftmost column. This forces $D = D' = I$ and $H = PBP'$. Since the product of the entries in each row of B is 1, and similarly for each column, the same must be true for H . This gives (16.11).

Hence we may suppose $k \in \{3, 4, 5, 6\}$; and our k MUB's are represented by the unitary matrices $I_5, U_0, U_1, \dots, U_{k-2}$ where

$$U_0 = B, \quad U_r = BM_r, \quad M_1, M_2, \dots, M_{k-2} \in \mathbb{M}_5; \quad \text{and} \\ \text{each } M_r \text{ has upper left corner entry 1.}$$

(Left-multiplication by arbitrary monomial matrices is not required here, since this will take our set to an equivalent set of MUB's.) Now each $M_r = [\lambda_{r,y}\delta_{x,\sigma_r(y)} : x, y \in F]$ where $|\lambda_{r,x}| = 1$ and σ_r is a permutation of F , for all $x \in F$ and $r \in \{0, 1, \dots, k-2\}$; moreover, $\lambda_{r,0} = \lambda_{0,x} = 1$, $\sigma_0(y) = y$ (the identity permutation) and $\sigma_r(0) = 0$ for all r .

Now the matrix $5U_r U_s^*$ has (x, y) -entry equal to

$$\sum_{z,v,w \in F} \zeta^{xz} \lambda_{r,v} \delta_{z,\sigma_r(v)} \delta_{w,\sigma_s(v)} \overline{\lambda_{s,v}} \zeta^{-wy} = \sum_{v \in F} \zeta^{x\sigma_r(v) - y\sigma_s(v)} \lambda_{r,v} \overline{\lambda_{s,v}},$$

which is required to have modulus equal to $\sqrt{5}$ whenever $r \neq s$ in $\{0, 1, \dots, k-2\}$. This means that

$$(16.12) \quad \begin{aligned} \text{for all } x, y \text{ in } F \text{ and } r \neq s, \quad 5 &= \left| \sum_{v \in F} \zeta^{x\sigma_r(v) - y\sigma_s(v)} \lambda_{r,v} \overline{\lambda_{s,v}} \right|^2 \\ &= \sum_{v,w \in F} \zeta^{x(\sigma_r(v) - \sigma_r(w)) - y(\sigma_s(v) - \sigma_s(w))} \lambda_{r,v} \overline{\lambda_{s,w}} \overline{\lambda_{r,v}} \lambda_{s,w}. \end{aligned}$$

Now specialize (16.12) to the case $r = y = 0$ and recall that $\sigma_0 = \text{id}$ and $\lambda_{0,x} = 1$ to obtain

$$(16.13) \quad \left| \sum_{w \in F} \zeta^{-xw} \lambda_{s,w} \right|^2 = \sum_{v,w \in F} \zeta^{x(v-w)} \lambda_{s,w} \overline{\lambda_{s,v}} = 5 \quad \text{whenever } x \in F \text{ and } s \neq 0.$$

Multiply both sides of (16.13) by ζ^{rx} , $r \in F$, and then sum over $x \in F$ to obtain

$$\sum_{v \in F} \lambda_{v+r} \overline{\lambda_v} = 5\delta_{r,0} \quad \text{for all } r \in F$$

where we abbreviate $\lambda_x := \lambda_{s,x}$ for fixed $s \neq 0$. That is, the circulant matrix $H = [\lambda_{x+y} : x, y \in F]$ is complex Hadamard! Normalizing H , we obtain

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \overline{\lambda_1}^2 \lambda_2 & \overline{\lambda_1 \lambda_2} \lambda_3 & \overline{\lambda_1 \lambda_3} \lambda_4 & \overline{\lambda_1 \lambda_4} \\ 1 & \overline{\lambda_1 \lambda_2} \lambda_3 & \overline{\lambda_2}^2 \lambda_4 & \overline{\lambda_2 \lambda_3} & \lambda_1 \overline{\lambda_2 \lambda_4} \\ 1 & \overline{\lambda_1 \lambda_3} \lambda_4 & \overline{\lambda_2 \lambda_3} & \lambda_1 \overline{\lambda_3}^2 & \lambda_0 \lambda_2 \overline{\lambda_3 \lambda_4} \\ 1 & \overline{\lambda_1 \lambda_4} & \lambda_1 \overline{\lambda_2 \lambda_4} & \lambda_2 \overline{\lambda_3 \lambda_4} & \lambda_3 \overline{\lambda_4}^2 \end{bmatrix},$$

using the fact that $\lambda_0 = \lambda_{s,0} = 1$. By (16.11), the product of the entries in each row of this matrix is 1. This says that each $\lambda_x = \lambda_{s,x}$ is a fifth root of unity. So there exist functions $f_s : F \rightarrow F$ satisfying $f_s(0) = 0$ and $\lambda_{s,x} = \zeta^{f_s(x)}$. Returning to (16.13), we now have

$$\left| \sum_{w \in F} \zeta^{f_s(w) - xw} \right| = \sqrt{5} \quad \text{for all } s \neq 0.$$

By Theorem 13.5, f_s is a quadratic function. Since $\lambda_{s,0} = \zeta^{f_s(0)} = 1$, we have $f_s(x) = a_s x^2 + b_s x$ for some $a_s, b_s \in F$. Returning to (16.12), but this time specializing to $r = 0$, we obtain

$$\left| \sum_{w \in F} \zeta^{a_s w^2 + (x+b_s)w + y\sigma_s(w)} \right| = \sqrt{5} \quad \text{for all } x, y \in F$$

where $a_s \neq 0$ for all $s \neq 0$. By Theorem 13.12, the permutation σ_s must be a first-degree polynomial: $\sigma_s(w) = m_s w + d_s$ for some $m_s, d_s \in F$ with $m_s \neq 0$. Now a straightforward computation shows that

$$U_s = BM_s = M'_s B_{a_s} \quad \text{where } M'_s = [\zeta^{d_s x} \delta_{m_s x + b_s, y} : x, y \in F] \in \mathbb{M}_5.$$

Again, we may dispense with the monomial matrices M'_s , using equivalence of MUBs, leaving $U_s = B_{a_s}$ for $s = 1, 2, \dots, k-2$. We also have $U_\infty = B_\infty = I_5$ and $U_0 = B_0 = B$; so our set of $k-2$ MUB's is (up to equivalence) a subset of the standard set. \square

Exercises 16.

1. The two groups of order 4 have character tables giving rise to Hadamard matrices

$$H_{4a} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}; \quad H_{4b} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

- (a) Show that H_{4a} and H_{4b} are not equivalent Hadamard matrices. That is, show that there do not exist unitary monomial matrices M, M' satisfying $H_{4b} = MH_{4a}M'$.
 - (b) Show that H_{4a} is equivalent to H_4 (from Example 16.2) for some choice of α ; and similarly for H_{4b} .
2. Exactly how many 'normalized' complex Hadamard matrices of order 5 are there? (See (16.9) and the comments which follow it.)

17. Weil's Bound

Fix a polynomial $g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_d x^d \in F[x]$ of degree $d \geq 2$, where $F = \mathbb{F}_q \supseteq K = \mathbb{F}_p$, $q = p^e$ and $\gcd(d, q) = 1$, $b_d \neq 0$; and consider the exponential sum

$$S_g = \sum_{a \in F} \zeta^{\text{Tr}_{F/K} g(a)} \in \mathbb{Z}[\zeta]$$

where $\zeta = \zeta_p$. Recall that $\text{Tr}_{F/K}$ is the absolute trace map

$$F \rightarrow K, \quad a \mapsto a + a^p + a^{p^2} + \dots + a^{p^{e-1}}.$$

Weil's bound (Theorem 13.2) is the assertion that

$$|S_g| \leq (d-1)\sqrt{q}.$$

We now outline key elements of the proof, using the machinery of L -functions introduced Section 12. We replace the choice of multiplicative function $\lambda : M \rightarrow \mathbb{C}$ used in Section 12 (designed for investigating Gauss sums and the Hasse-Davenport relations) by a new choice $\lambda = \lambda_g$; but everything in Section 12 up to (12.6) applies here as well. While we omit some details in the proof of Weil's bound, these can be found in other sources. The details, as found in [LN], [Sc], are elementary if somewhat technical.

Our rationale for naming the fixed polynomial $g(x)$ (above) is to reserve the name $f \in M$ for an arbitrary monic polynomial as in our previous generalities regarding L -functions. As before, M is the multiplicative monoid of monic polynomials in $F[x]$. Recall that all nonzero ideals $\mathcal{A} \subseteq \mathcal{O} = F[x]$ are principal, having the form $\mathcal{A} = (f)$ for some $f \in M$. We are ready to introduce our new choice of multiplicative function $\lambda(\mathcal{A}) = \lambda(f) = \lambda_g(f)$ which depends on the choice of given polynomial g above.

Recall that it suffices to define $\lambda(f)$ for $f \in P$ (i.e. f monic irreducible), then extend to the monoid M using unique factorization in $F[x]$. So given $f \in P_k$, recall that $E = \mathbb{F}_{q^k}$ is the splitting field of f over F , thus:

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_k), \quad \text{some distinct } r_1, r_2, \dots, r_k \in E.$$

We define

$$\lambda(f) = \lambda_g(f) = \zeta^{\text{Tr}_{F/K}[g(r_1)+g(r_2)+\cdots+g(r_k)]}.$$

We must of course show that this definition makes sense! Obviously $\sum_i g(r_i) \in E$; but since every F -automorphism σ of E permutes the n roots of f by Theorem A5.3, σ permutes the k terms in $\sum_i g(r_i)$. (Recall: the Galois group $G(E/F)$ is cyclic and $\sigma(a) = a^{q^j}$ for some $j \in \{0, 1, 2, \dots, k-1\}$). Hence $\sigma(\sum_i g(r_i)) = \sum_i g(r_i)$. By Galois theory, this means that $\sum_i g(r_i) \in F$, where F is the domain of our trace map $\text{Tr}_{F/K}$.

We will denote the associated L -function by $L_g(s) := L_{\lambda_g}(s)$. As before, the key step is proving that the coefficient of z^n in the series expansion of $L_g(s)$ vanishes for large n (see (12.5)), thus forcing the L -function to be a polynomial in z .

Recall that $M_n \subset M$ is the set of monic polynomials $f(x) \in F[x]$ of degree n .

Lemma 17.1. If $n \geq d$, then $\sum_{f \in M_n} \lambda(f) = 0$.

Proof. Each $f \in M_n$ has the form

$$f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n = (x - r_1)(x - r_2) \cdots (x - r_n)$$

where $e_i = e_i(r_1, r_2, \dots, r_n) \in F$ are elementary symmetric polynomials in the roots; see Appendix A7. Now

$$g(r_1) + g(r_2) + \cdots + g(r_n) = \sum_{j=0}^d \sum_{i=1}^n b_j r_i^j = \sum_{j=0}^d b_j m_j$$

where

$$m_j = m_j(r_1, r_2, \dots, r_n) = r_1^j + r_2^j + \dots + r_n^j$$

are the moment polynomials in the roots. (Thus $m_0 = n$, $m_1 = e_1$, $m_2 = e_1^2 - 2e_2$, etc. as in Theorem A7.3.) By Corollary A7.4, we have

$$m_d = (-1)^{d-1} d e_d + h(e_1, e_2, \dots, e_{d-1})$$

for some polynomial $h(t_1, t_2, \dots, t_{d-1}) \in F[t_1, t_2, \dots, t_{d-1}]$. Thus

$$\begin{aligned} \sum_{i=1}^n g(r_i) &= b_0 m_0 + b_1 m_1 + b_2 m_2 + \dots + b_{d-1} m_{d-1} + b_d [(-1)^{d-1} d e_d + h(e_1, e_2, \dots, e_{d-1})] \\ &= (-1)^{d-1} d b_d e_d + \tilde{h}(e_1, e_2, \dots, e_{d-1}) \end{aligned}$$

for some polynomial $\tilde{h}(e_1, e_2, \dots, e_{d-1}) \in F[e_1, e_2, \dots, e_{d-1}]$ (whose coefficients depend on the fixed polynomial g). Thus

$$\begin{aligned} \sum_{f \in M_n} \lambda(f) &= \sum_{f \in M_n} \zeta^{\text{Tr}_{F/K}[g(r_1) + g(r_2) + \dots + g(r_n)]} \\ &= \sum_{e_1, e_2, \dots, e_n \in F} \zeta^{\text{Tr}_{F/K}[(-1)^{d-1} d b_d e_d + \tilde{h}(e_1, e_2, \dots, e_{d-1})]} && \text{(summing over } f \in M_n \\ & && \text{amounts to summing over} \\ & && \text{choices for its coefficients)} \\ &= q^{n-d} \sum_{e_1, e_2, \dots, e_d \in F} \zeta^{\text{Tr}_{F/K}[(-1)^{d-1} d b_d e_d + \tilde{h}(e_1, e_2, \dots, e_{d-1})]} && \text{(the summand is independent} \\ & && \text{of } e_{d+1}, \dots, e_n \in F) \\ &= q^{n-d} \sum_{e_d \in F} \zeta^{(-1)^{d-1} \text{Tr}_{F/K}(d b_d e_d)} \sum_{e_1, e_2, \dots, e_{d-1} \in F} \zeta^{\text{Tr}_{F/K} \tilde{h}(e_1, e_2, \dots, e_{d-1})} = 0 \end{aligned}$$

since $d b_d \neq 0$ and the map $x \mapsto \zeta^{\text{Tr}_{F/K}(d b_d x)}$ is a nontrivial additive character of F by Theorem A1.7(ii). This last step makes essential use of the hypothesis $p \nmid d$. \square

By (12.5), $L_g(s)$ is a polynomial in z of degree at most $d-1$, so

$$L_g(s) = (1 - \omega_1 z)(1 - \omega_2 z) \cdots (1 - \omega_{d-1} z)$$

for some $\omega_1, \omega_2, \dots, \omega_{d-1} \in \mathbb{C}$. Now

$$\sum_{i=1}^{d-1} \ln(1 - \omega_i z) = \ln L_g(s) = - \sum_{k=1}^{\infty} \sum_{f \in P_k} \ln(1 - \lambda(f) z^k)$$

and so

$$\begin{aligned} - \sum_{n=1}^{\infty} (\omega_1^n + \dots + \omega_{d-1}^n) z^n &= - \sum_{i=1}^{d-1} \frac{\omega_i z}{1 - \omega_i z} = z \frac{L'_g(z)}{L_g(z)} = \sum_{k=1}^{\infty} \sum_{f \in P_k} \frac{k \lambda(f) z^k}{1 - \lambda(f) z^k} \\ &= \sum_{k=1}^{\infty} \sum_{f \in P_k} \sum_{r=1}^{\infty} k \lambda(f)^r z^{r k} = \sum_{n=1}^{\infty} \sum_{k|n} \sum_{f \in P_k} k \lambda(f)^{n/k} z^n. \end{aligned}$$

Equating coefficients gives

$$-(\omega_1^n + \cdots + \omega_{d-1}^n) = \sum_{k|n} \sum_{f \in P_k} k\lambda(f)^{n/k}$$

for all $n \geq 1$. We will show that the latter double sum is simply $\sum_{\alpha \in E} \zeta^{\text{Tr}_{E/K} g(\alpha)}$ where $E = \mathbb{F}_{q^n}$. Given $\alpha \in E$, let $f(x)$ be its minimal polynomial over F , so $\deg f(x) = k = [F[\alpha] : F]$ which divides $[E : F] = n$; moreover in this case Theorem 3.8 gives

$$f(x) = (x - \alpha)(x - \alpha^q)(x - \alpha^{q^2}) \cdots (x - \alpha^{q^{k-1}})$$

and we can group together the k terms in our sum arising from the same minimal polynomial $f(x)$ to get

$$\begin{aligned} \sum_{\alpha \in E} \zeta^{\text{Tr}_{E/K} g(\alpha)} &= \sum_{k|n} \sum_{f \in P_k} [\zeta^{\text{Tr}_{E/K} g(\alpha)} + \zeta^{\text{Tr}_{E/K} g(\alpha^q)} + \cdots + \zeta^{\text{Tr}_{E/K} g(\alpha^{q^{k-1}})}] \\ &= \sum_{k|n} \sum_{f \in P_k} k\zeta^{\text{Tr}_{E/K} g(\alpha)} \quad (\text{Corollary A5.14}) \\ &= \sum_{k|n} \sum_{f \in P_k} k(\zeta^{\text{Tr}_{F[\alpha]/K} g(\alpha)})^{n/k} \quad (\text{Corollary A1.10}) \\ &= \sum_{k|n} \sum_{f \in P_k} k(\zeta^{\text{Tr}_{F/K} \text{Tr}_{F[\alpha]/F} g(\alpha)})^{n/k} \quad (\text{Theorem A1.8}) \\ &= \sum_{k|n} \sum_{f \in P_k} k(\zeta^{\text{Tr}_{F/K} [g(\alpha) + g(\alpha^q) + \cdots + g(\alpha^{q^{k-1}})]})^{n/k} \quad (\text{Theorem 3.8}) \\ &= \sum_{k|n} \sum_{f \in P_k} k(\zeta^{\text{Tr}_{F/K} [g(\alpha) + g(\alpha^q) + \cdots + g(\alpha^{q^{k-1}})]})^{n/k} \quad (\text{since } g(x) \in F[x]; \\ &\quad \text{see Theorem A5.3}) \\ &= \sum_{k|n} \sum_{f \in P_k} k\lambda(f)^{n/k}. \end{aligned}$$

Thus

Corollary 17.2. Let $F = \mathbb{F}_q \supseteq K = \mathbb{F}_p$ be a field of order $q = p^e$, and let $g(x) \in F[x]$ be a polynomial of degree $d \geq 2$ with $\gcd(d, q) = 1$. Then there exist complex numbers $\omega_1, \dots, \omega_{d-1}$ such that $\sum_{\alpha \in E} \zeta^{\text{Tr}_{E/K} g(\alpha)} = -(\omega_1^n + \cdots + \omega_{d-1}^n)$ for every $d \geq 1$ where $E = \mathbb{F}_{q^n}$. \square

Now Schmidt [Sc] gives an elementary (but rather technical) proof of

$$(17.3) \quad \text{Each of the complex numbers } \omega_1, \omega_2, \dots, \omega_{d-1} \text{ in Corollary 17.2 satisfies } |\omega_i| = \sqrt{p}.$$

Using (17.3) together with Corollary 17.2, we have

$$|S_g| = \left| \sum_{\alpha \in E} \zeta^{\text{Tr}_{E/K} g(\alpha)} \right| = |\omega_1^n + \omega_2^n + \cdots + \omega_{d-1}^n| \leq (d-1)\sqrt{p}^n = (d-1)q^n$$

which is Weil's bound. In place of Schmidt's technical argument, Lidl and Niederreiter [LN] substitute a slightly less technical (but also elementary) argument proving $|\omega_i| \leq \sqrt{p}$. This is also sufficient to establish Weil's bound, as is clear from the argument above; but it is less satisfying in that it falls short of proving the equality in (17.3). We did not feel so compelled to complete the proof of Weil's bound as to devote many more technical pages to the goal, having already described what we view as the nicest part of the proof.

Example 17.4: Quadratic Exponential Sum. Let $F = \mathbb{F}_p$ where p is an odd prime, and take $g(x) = x^2$. Here $d = 2$ which does not divide p . If $E = \mathbb{F}_q$, $q = p^n$ then by Theorem 13.3 and Corollary 12.11,

$$\omega_1^n = -G(\chi^E) = \begin{cases} (-\sqrt{p})^n, & \text{if } p \equiv 1 \pmod{4}; \\ (-i\sqrt{p})^n, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Evidently $\omega_1 = -\sqrt{p}$ or $-i\sqrt{p}$ according as $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$. Note that (17.3) is satisfied. Replacing $g(x)$ with another quadratic polynomial give a similar results.

Exercises 17.

1. Let $F = \mathbb{F}_3$ and $E = \mathbb{F}_q$ where $q = 3^n$, and let $g(x) = x^5 + x \in F[x]$. Note that $d=5$ which is relatively prime to q . Here $\zeta = \zeta_3 = \omega$ and all exponential sums have values in the Eisenstein integers $\mathbb{Z}[\omega]$.
 - (a) Compute a table of values of $g(a)$ for $a \in \mathbb{F}_9$. It is convenient to take $\mathbb{F}_9 = \mathbb{F}_3[i]$ where $i = \sqrt{-1}$.
 - (b) Using (a), compute $\sum_{a \in E} \omega^{\text{Tr}_{E/F} g(a)} \in \mathbb{Z}[\omega]$ for $n = 1, 2$.
 - (c) Equating the sum in (b) to $-\omega_1^n - \omega_2^n$, obtain two equations in two unknowns $\omega_1, \omega_2 \in \mathbb{C}$. Solve for ω_1 and ω_2 .
 - (d) Does the equality of (17.3) hold? Explain.
 - (e) Use Corollary 17.2 to evaluate the exponential sum for $n = 1, 2, 3, 4, 5, 6$.
 - (f) Half of the values listed in (e) are zero. Give a very simple explanation for this fact. (*Hint:* Comments immediately following the statement of Theorem 11.7 use similar reasoning.)

Appendix A1: Fields and Extensions

See e.g. [Sa], [Mc] for details on fields and extensions.

Recall that a **field** is a commutative ring F with identity, in which every nonzero element is a unit (i.e. has a multiplicative inverse). The key feature which distinguishes fields from more general commutative rings, is that it is closed not only under addition, subtraction and multiplication, but also under division (meaning that if $a, b \in F$ with $a \neq 0$, then the equation $ax = b$ has a unique solution $x = \frac{b}{a} \in F$). Examples of commutative rings with identity, which are *not* fields, include: \mathbb{Z} , $R[x]$ where R is any commutative ring with identity, and $F^n = F \oplus \cdots \oplus F$ ($n \geq 2$ copies, with componentwise addition and multiplication). Here $R[x]$ is the ring of polynomials in an indeterminate x with coefficients in R . Examples of fields include: \mathbb{C} , \mathbb{Q} , \mathbb{R} , and the field $F(x)$ of rational functions in an indeterminate x with coefficients in F . Here $F(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x] \text{ with } g(x) \neq 0 \right\}$.

An **extension of fields** is a pair of fields $E \supseteq F$ where F is a subring (and hence a subfield) of E . In this case, it is clear from the axioms that E is also a vector space over F ; and so we may speak of the dimension of this vector space. We call this dimension the **degree** of the extension, denoted $[E : F]$. Here $[E : F] \geq 1$, where equality holds iff $E = F$. For example, $\mathbb{C} \supset \mathbb{R}$ is an extension of degree $[\mathbb{C} : \mathbb{R}] = 2$ (a **quadratic extension**) with basis $\{1, i\}$, and the extension $\mathbb{R} \supset \mathbb{Q}$ has infinite degree. A **finite extension** is an extension of finite degree (regardless of whether the fields themselves are finite or infinite). A **tower** of fields is a chain of extension fields $E_n \supseteq E_{n-1} \supseteq \cdots \supseteq E_1 \supseteq E_0$. Every such tower has degree $[E_n : E_0] = \prod_{i=1}^n [E_i : E_{i-1}]$ as one proves by induction on n , using the following result. We refer to this result as the **transitivity of degrees** for extension fields.

Theorem A1.1. If $K \supseteq E \supseteq F$ is a tower of fields, then $[K : F] = [K : E][E : F]$.

Proof. Suppose $\{\alpha_1, \dots, \alpha_m\}$ is a basis for K over E , and $\{\beta_1, \dots, \beta_n\}$ is a basis for E over F . It is easy to see that $\{\alpha_i \beta_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for K over F . Indeed, every $\alpha \in K$ can be uniquely expressed as $\alpha = \sum_{i=1}^m a_i \alpha_i$ with $a_i \in E$; and we can uniquely express $a_i = \sum_{j=1}^n b_{ij} \beta_j$ with $b_{ij} \in F$. This gives a unique expression $\alpha = \sum_{i=1}^m \sum_{j=1}^n b_{ij} \alpha_i \beta_j$ with $b_{ij} \in F$ as required. \square

Although we have proved Theorem A1.1 only in the case of finite degree, one similarly proves the general case (with the obvious convention that $[K : F] = \infty$ iff at least one of $[K : E]$ or $[E : F]$ is infinite. Theorem A1.1 should be seen as the field-theoretic analogue of the statement $[G : K] = [G : H][H : K]$ for chains of subgroups $G \geq H \geq K$.

The **characteristic** of a field F , denoted $\text{char } F$, equals the minimum positive integer n such that $1 + 1 + \cdots + 1 = 0$ (with n 1's), if such an n exists; otherwise we say F has characteristic zero and we write $\text{char } F = 0$. For a field F of positive characteristic, $\text{char } F = p$ must be prime. This fact is proved by an obvious generalization of the following explanation why $\text{char } F \neq 6$: otherwise

$$0 = 1 + 1 + 1 + 1 + 1 + 1 = (1 + 1)(1 + 1 + 1)$$

which yields either $1 + 1 = 0$ or $1 + 1 + 1 = 0$ in F , contradicting the minimality of $\text{char } F$. For every extension $E \supseteq F$, it is clear that E and F have the same characteristic. Moreover, every field F has a unique smallest subfield K , called the **prime subfield** of F ; and this field is isomorphic to \mathbb{F}_p , the field prime order p , if $\text{char } F = p$; or \mathbb{Q} , in the case $\text{char } F = 0$.

Theorem A1.2. Let $E \supseteq F$ be an extension of fields., and let $\theta \in E$. Then the following three conditions are equivalent:

- (i) θ is a root of a nonzero polynomial $f(x) \in F[x]$;
- (ii) the powers $1, \theta, \theta^2, \theta^3, \dots$ are linearly dependent over F ;
- (iii) $F[\theta]$ is a field (hence equal to $F(\theta)$, its field of quotients).

Assuming these conditions hold, there is a unique smallest degree monic polynomial $m(x) \in F[x]$ satisfying $m(\theta) = 0$; and this polynomial $m(x)$ is irreducible in $F[x]$. In fact $m(x) \in F[x]$ is the unique monic irreducible polynomial having θ as a root; and a polynomial $f(x) \in F[x]$ satisfies $f(\theta) = 0$ iff $f(x)$ is divisible by $m(x)$ in $F[x]$.

Under the conditions of Theorem A1.2, we say θ is **algebraic** over F ; and $\text{Irr}_{\theta, F}(x) := m(x)$ is the **minimal polynomial** of θ over F . Moreover, θ is **algebraic of degree n** where $n = \deg m(x) = [E : F]$.

Proof. Assuming (ii), there is a linear combination

$$a_0 + a_1\theta + a_2\theta^2 + \cdots + a_n\theta^n = 0$$

for some $a_0, \dots, a_n \in F$, not all zero; and this proves (i).

Assuming (i), the subset $J \subseteq F[x]$ consisting of all $f(x) \in F[x]$ such that $f(\theta) = 0$, is a nonzero ideal. Choose a nonzero element $m(x) \in J$ of smallest degree; and without loss of generality, $m(x)$ is monic. Now J contains the principal ideal $(m(x)) = \{g(x)m(x) : g(x) \in F[x]\} \subseteq J$. By the Division Algorithm, it is easy to see that equality holds: $J = (m(x))$. If $m(x) = m_1(x)m_2(x)$ where $m_1(x), m_2(x) \in F[x]$, then either $m_1(x)$ or $m_2(x)$ must have θ as a root; and by minimality of $\deg m(x)$, one of the factors $m_i(x)$ must be a nonzero constant; so $m(x)$ is irreducible in $F[x]$. Now the ideal $(m(x)) \subset F[x]$ is maximal; so the quotient ring $F[x]/(m(x))$ is a field. Also the evaluation map $F[x] \rightarrow F[\theta]$, $f(x) \mapsto f(\theta)$ is

a surjective ring homomorphism; and its kernel is $J = (m(x))$. So the First Isomorphism Theorem for Rings gives

$$F[\theta] \cong F[x]/(m(x)),$$

a field. This proves (iii), and later assertions regarding $m(x)$ follow as well.

Finally, suppose (iii) holds; and we must prove (ii). We may suppose $\theta \neq 0$, otherwise there is nothing to prove. By (iii), θ has a multiplicative inverse in $F[\theta]$, so there exist $m \geq 0$ and $b_0, b_1, \dots, b_m \in F$ such that

$$(b_0 + b_1\theta + b_2\theta^2 + \dots + b_m\theta^m)\theta = 1.$$

After expanding and moving all terms to one side, we obtain (ii) as required. \square

An extension $E \supseteq F$ is **algebraic** if every element of E is algebraic over F .

Corollary A1.3. Every finite extension is algebraic.

Proof. Let $E \supseteq F$ be a finite extension of degree $n = [E : F]$, and let $\theta \in E$. Then the $n + 1$ elements $1, \theta, \theta^2, \dots, \theta^n \in E$ must be linearly dependent over F ; so θ is algebraic over F (of degree at most n). \square

Corollary A1.4. Let $E \supseteq F$ be an extension of fields, and suppose the elements $\alpha, \beta \in E$ are algebraic over F . Then $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are algebraic over F . Also if $\beta \neq 0$ then $\frac{\alpha}{\beta}$ is algebraic over F .

Proof. Since α is algebraic over F , we have a finite extension field $L := F[\alpha] \supseteq F$ and so $[L : F] < \infty$. Since β is algebraic over F , it is algebraic over L ; so $L[\beta] \supseteq L$ is a finite extension. Now $[L[\beta] : F] = [L[\beta] : L][L : F] < \infty$, so the extension $L[\beta] \supseteq F$ is algebraic. So the elements $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in F[\alpha, \beta] = L[\beta]$ are algebraic over F . \square

Thus the set of all elements of an extension $E \subseteq F$ which are algebraic over F , forms an intermediate subfield. In particular, \mathbb{C} has a subfield \mathbb{A} consisting of all complex numbers that are algebraic over \mathbb{Q} . Note that \mathbb{A} is **algebraically closed** (i.e. every nonconstant polynomial $f(t) \in \mathbb{A}[t]$ has a root in \mathbb{A}); and the extension $\mathbb{A} \supset \mathbb{Q}$ is algebraic (i.e. every element of \mathbb{A} is algebraic over \mathbb{Q}); so \mathbb{A} is the **algebraic closure** of \mathbb{Q} . Evidently \mathbb{A} contains all complex roots of unity; but \mathbb{A} is not generated by the roots of unity. Since $[\mathbb{A} : \mathbb{Q}] = \infty$, the converse of Corollary A1.3 evidently fails. Note also that \mathbb{A} is a proper subfield of \mathbb{C} , since \mathbb{C} is uncountable whereas \mathbb{A} is countable.

Corollary A1.5. Let $K \supseteq E \supseteq F$ be a tower of extensions, where $K \supseteq E$ is algebraic and $E \supseteq F$ is algebraic. Then $K \supseteq F$ is algebraic.

By induction, Corollary A1.5 obviously extends to towers of extensions of arbitrary finite length.

Proof of Corollary A1.5. Let $\theta \in K$. By hypothesis, θ is algebraic over E , so there exist $n \geq 1$ and $a_0, a_1, \dots, a_{n-1} \in E$ such that

$$\theta^n + a_{n-1}\theta^{n-1} + \dots + a_1\theta + a_0 = 0.$$

Since $a_0 \in E$ is algebraic over F , $F[a_0] \supseteq F$ is a finite extension. Also $a_1 \in E$ is algebraic over F so it is algebraic over $F_0 := F[a_0]$, which means that $F_1 := F_0[a_1] = F[a_0, a_1]$ is a finite extension of F . Continuing in this way, we come to a finite extension field $F_{n-1} := F[a_0, a_1, \dots, a_{n-1}] \supseteq F$. The relation above shows that θ is algebraic over F_{n-1} , so it generates a finite extension field $F_{n-1}[\theta] \supseteq F_{n-1}$. Again using transitivity of extensions, $[F_{n-1}[\theta] : F] < \infty$ and so by Corollary A1.3, θ is algebraic over F . \square

Matrix Representations of Field Extensions

Let $E \supseteq F$ be a field extension of degree n . Then E is isomorphic to a subring of the ring of $n \times n$ matrices over F , which we denote by $F^{n \times n}$. To see this, note that every $\alpha \in E$ defines an F -linear transformation $T_\alpha : E \rightarrow E$, $x \mapsto \alpha x$. Now fix a basis of E over F ; and denote by $M(\alpha)$ the matrix of T_α with respect to the chosen basis. Now $M : E \rightarrow F^{n \times n}$ is clearly an injective, F -linear, and $M(\alpha\beta) = M(\alpha)M(\beta)$, $M(\alpha+\beta) = M(\alpha) + M(\beta)$. So the image of $M : E \rightarrow F^{n \times n}$ is a subring isomorphic to E . Define the **norm** and **trace** of α (with respect to the extension $E \supseteq F$) as the elements

$$N_{E/F} \alpha = \det M(\alpha), \quad \text{Tr}_{E/F} \alpha = \text{tr } M(\alpha)$$

respectively, where $\text{tr} : F^{n \times n} \rightarrow F$ is the usual matrix trace (the sum of the diagonal entries). Note that both of these are maps $E \rightarrow F$. They do not depend on the choice of bases used, since they are the determinant and the trace of T_α , admitting a basis-free description. In the case where F is the prime field of E (i.e. its minimal subfield), the norm and trace are called the **absolute norm** and **absolute trace**.

Example A1.6: The Complex Numbers. Take $\{1, i\}$ as a basis for \mathbb{C} over \mathbb{R} . The matrix of $\alpha = a + bi$ ($a, b \in \mathbb{R}$) with respect to this basis is $M(\alpha) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. The norm and trace are given by $N_{\mathbb{C}/\mathbb{R}} \alpha = a^2 + b^2$ and $\text{Tr}_{\mathbb{C}/\mathbb{R}} \alpha = 2a$.

Theorem A1.7. Let $E \supseteq F$ be a finite extension of fields. Write $N = N_{E/F}$, $\text{Tr} = \text{Tr}_{E/F}$. For all $a, b \in E$ we have

- (i) $N(ab) = N(a)N(b)$. Moreover $N(a) = 0$ iff $a = 0$.
- (ii) $\text{Tr}(a+b) = \text{Tr} a + \text{Tr} b$. The map $\text{Tr} : E \rightarrow F$ is an F -linear functional. A bilinear form on E is defined by $(a, b) \mapsto \text{Tr}(ab)$. If E (and F) have characteristic zero or are finite fields, then this bilinear form is nondegenerate and symmetric, i.e. $\text{Tr}(ab) = \text{Tr}(ba)$; and $b = 0$ is the only element satisfying $\text{Tr}(ab) = 0$ for all $a \in E$.

Proof. The identities $N(ab) = N(a)N(b)$ and $\text{Tr}(a+b) = \text{Tr} a + \text{Tr} b$ follow from $T_{ab} = T_a T_b$ and $T_{a+b} = T_a + T_b$ using basic properties of determinant and trace for linear transformations. Also $N(1) = \det I = 1$; so if $a \in E^\times$ then $N(a)N(a^{-1}) = N(1) = 1$. Finally, suppose $\text{Tr}(ab) = 0$ for all $a \in E$; we must show that $b = 0$. It suffices to find $c \in E$ satisfying $\text{Tr} c \neq 0$; for then we may take $a = \frac{c}{b}$ whenever $b \neq 0$. In characteristic zero, $\text{Tr} 1 = n = [E : F] \neq 0$ as required. In the finite case $F = \mathbb{F}_q$ and $E = \mathbb{F}_{q^n}$, an extension of finite fields of degree $[E : F] = n$, $\text{Tr} a = a + a^q + a^{q^2} + \cdots + a^{q^{n-1}}$ by Theorem 3.8. If $\text{Tr} c = 0$ for all $c \in E$, then the polynomial $x^{q^{n-1}} + \cdots + x^q + x \in F[x]$ has q^n roots in E , and this number exceeds the degree q^{n-1} of the polynomial, a contradiction; so once again there exists $c \in E$ with $\text{Tr} c \neq 0$ as required. \square

Regarding the necessity of the additional assumption in Theorem A1.7(ii), see Example A4.3.

The matrix representation gives the impression of making the arithmetic of field extensions more concrete or facilitating implementation. On the contrary, it is *not practical* for implementation (since it requires storing n^2 matrix entries for each element of E , rather than E in the usual representation). For computer implementation, polynomial arithmetic (modulo an irreducible polynomial) is still the best. But the matrix representation is surprisingly useful as a theoretical device for explaining certain properties of field extensions.

For example, consider the ring $R = F^{n \times n}$, the ring of $n \times n$ matrices over F ; and let $R^{m \times m}$ be the ring of $m \times m$ matrices over R . Then we have the isomorphism $R^{m \times m} \cong F^{mn \times mn}$ which, although not difficult to prove, is still rather subtle and somewhat surprising. And replacing R by the subring $S = \{M(\alpha) : \alpha \in E\} \subseteq R$ using the matrix representation of an extension $E \supseteq F$ of degree n as above, the isomorphism $E \cong S \subseteq R$ induces an isomorphism between the ring $E^{m \times m}$ of $m \times m$ matrices over E , and the subring $M(E^{m \times m}) \subseteq F^{mn \times mn}$ defined by replacing each entry of a matrix $A \in E^{m \times m}$ by its matrix representation in S :

$$\underbrace{A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mm} \end{bmatrix}}_{\text{an } m \times m \text{ matrix over } E} \mapsto \underbrace{M(A) = \begin{bmatrix} M(\alpha_{11}) & M(\alpha_{12}) & \cdots & M(\alpha_{1m}) \\ M(\alpha_{21}) & M(\alpha_{22}) & \cdots & M(\alpha_{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ M(\alpha_{m1}) & M(\alpha_{m2}) & \cdots & M(\alpha_{mm}) \end{bmatrix}}_{\text{an } mn \times mn \text{ matrix over } F}$$

This map preserves more than the ring operations ‘+’ and ‘×’; it also respects traces and determinants: for all $A \in E^{m \times m}$,

$$\mathrm{Tr}_{E/F}(\mathrm{tr} A) = \mathrm{tr} M(A) \quad \text{and} \quad \mathrm{N}_{E/F}(\det A) = \det M(A).$$

(We continue to distinguish the usual matrix trace ‘tr’ and the trace ‘Tr’ for field extensions using lower and upper case, respectively. Note the necessity of using the norm and trace maps $E \rightarrow F$ since matrices on the left are over E ; matrices on the right are over F .) The first formula is easy to see by adding diagonal entries on both sides; the second formula can be proved by first verifying it for elementary matrices $A \in E^{m \times m}$, then using the multiplicative property to extend to the general case).

Now given a tower of finite extensions $K \supseteq E \supseteq F$, we have three trace maps and three norm maps

$$\begin{array}{ccc} & \mathrm{Tr}_{K/F} & \\ & \curvearrowright & \\ K & \xrightarrow{\mathrm{Tr}_{K/E}} & E \xrightarrow{\mathrm{Tr}_{E/F}} F \\ & \curvearrowleft & \end{array} \qquad \begin{array}{ccc} & \mathrm{N}_{K/F} & \\ & \curvearrowright & \\ K & \xrightarrow{\mathrm{N}_{K/E}} & E \xrightarrow{\mathrm{N}_{E/F}} F \\ & \curvearrowleft & \end{array}$$

The **transitivity** of norm and trace maps is the assertion that these diagrams commute:

Theorem A1.8. For a tower $K \supseteq E \supseteq F$ as above, $\mathrm{Tr}_{K/F} = \mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{K/E}$ and $\mathrm{N}_{K/F} = \mathrm{N}_{E/F} \circ \mathrm{N}_{K/E}$.

Proof. Use the observations above, restricting the matrix $A \in E^{m \times m}$ to lie in the matrix representation of K , where $m = [K : E]$. \square

When representing a finite field extension $E \supseteq F$ as a ring of $n \times n$ matrices over F , sometimes we are led to consider the full characteristic polynomial of each matrix $M(\alpha)$, $\alpha \in E$ (i.e. rather than just the trace and norm, which are obtained from just two coefficients in this polynomial). Here we may use

Theorem A1.9. Let $K \supseteq F$ be a finite extension of fields, and let $\alpha \in K$. Denote $E = F[\alpha]$, $n = [E : F]$ and $m = [K : E]$ so that $[K : F] = mn$. Multiplication by α gives F -linear maps $E \rightarrow E$ and $K \rightarrow K$ with corresponding matrix representations $M_E(\alpha) \in F^{n \times n}$ and $M_K(\alpha) \in F^{mn \times mn}$ respectively. The characteristic polynomial of $M_K(\alpha)$ is $\det(xI - M_K(\alpha)) = h(x)^m$ where $h(x) = \det(xI - M_E(\alpha))$. Moreover, $h(x)$ is the minimal polynomial of α over F .

Proof. We may use $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ as a basis for E over F , and let $\{\beta_1, \beta_2, \dots, \beta_m\}$ be a basis for K over E (as in the proof of Theorem A1.1). The matrix of T_α with respect to the basis $\{\alpha^j \beta_i : 1 \leq i \leq m, 1 \leq j \leq n\}$ is $M_K(\alpha) = I_m \otimes M_E(\alpha)$ where $M_E(\alpha)$ is the $n \times n$

companion matrix of $h(x)$. The result follows. \square

Corollary A1.10. Under the hypotheses of Theorem A1.9, $\text{Tr}_{K/F} \alpha = m \text{Tr}_{E/F} \alpha$ and $\text{N}_{K/F} \alpha = (\text{N}_{E/F} \alpha)^m$. \square

Appendix A2: Polynomials and Irreducibility

Every finitely generated additive subgroup of \mathbb{Q} is generated by a single element. This says that if r_1, \dots, r_n are rational numbers, then there exists $r \in \mathbb{Q}$ such that

$$\mathbb{Z}r_1 + \mathbb{Z}r_2 + \cdots + \mathbb{Z}r_n = \mathbb{Z}r.$$

We will assume r_1, \dots, r_n are not all zero (otherwise one clearly takes $r = 0$). Now to find r , first find the smallest positive integer b such that $br_i \in \mathbb{Z}$ for all i (so b is the least common denominator). Then take $a = \gcd(br_1, \dots, br_n)$. Recall that there exist integers k_1, \dots, k_n such that

$$k_1 \cdot br_1 + k_2 \cdot br_2 + \cdots + k_n \cdot br_n = a$$

and this is the least positive element in $\mathbb{Z}br_1 + \cdots + \mathbb{Z}br_n$. Dividing both sides by b , we get $r := \frac{a}{b}$ as the least positive integer in the additive subgroup $\mathbb{Z}r_1 + \cdots + \mathbb{Z}r_n \subset \mathbb{Q}$.

Again assuming r_1, \dots, r_n are not all zero, the additive subgroup $\mathbb{Z}r_1 + \cdots + \mathbb{Z}r_n \subset \mathbb{Q}$ is infinite cyclic. Denote by $r = \text{wt}(r_1, \dots, r_n) \in \mathbb{Q}$ its unique positive generator (so that $\pm r$ are the two choices of generator). Also for any nonzero polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$, define the **weight** of $f(x)$ by

$$\text{wt } f = \text{wt } f(x) = \text{wt}(a_0, a_1, \dots, a_n).$$

Lemma A2.1. Suppose $f(x), g(x), h(x) \in \mathbb{Q}[x]$ are nonzero polynomials.

- (i) $f(x) \in \mathbb{Z}[x]$ iff $\text{wt } f \in \mathbb{Z}$; and in this case, the weight of f is simply the greatest common divisor of its coefficients.
- (ii) $\text{wt}(fg) = \text{wt } f + \text{wt } g$.
- (iii) Assume $f(x) = g(x)h(x)$. If at least two of the polynomials f, g, h are monic with integer coefficients, then so is the third.

Proof. (i) Let a_0, a_1, \dots, a_n be the coefficients in $f(x)$; and let $a = \text{wt } f$. Since $\mathbb{Z}a = \mathbb{Z}a_0 + \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$, clearly $a \in \mathbb{Z}$ iff every $a_i \in \mathbb{Z}$. The remaining assertion uses only well-known properties of ideals in \mathbb{Z} , using the extended Euclidean algorithm (see also the explanations above).

(ii) Let $r = \text{wt } f$, $s = \text{wt } g$, $t = \text{wt}(fg)$ so that

$$f(x) = ru_f(x), \quad g(x) = su_g(x), \quad f(x)g(x) = tu_{fg}(x)$$

where each of the three polynomials $u_f(x), u_g(x), u_{fg}(x) \in \mathbb{Z}[x]$ has weight 1. Reducing the fraction $\frac{rs}{t} \in \mathbb{Q}$ to lowest terms as $\frac{rs}{t} = \frac{a}{b}$ where a, b are relatively prime positive integers, we obtain

$$(A2.2) \quad bu_{fg}(x) = au_f(x)u_g(x).$$

If $b > 1$ then there exists a prime p dividing b , with $p \nmid a$. Reducing both sides of (A2.2) modulo p , we find a product of two nonzero polynomials in $\mathbb{F}_p[x]$ equal to the zero polynomial. This is a contradiction, since $F[x]$ has no zero divisors (by comparing leading terms on both sides) for any field F . This shows that $b = 1$. Now the right hand side of (A2.2) clearly has weight divisible by a . Since the left hand side has weight 1, we obtain $a = 1$. This gives $rs = t$ as required.

(iii) If $g(x), h(x)$ are monic with integer coefficients, then clearly so is their product. Now suppose $f(x), g(x) \in \mathbb{Z}[x]$ are monic with $f(x) = g(x)h(x)$. Since $\text{wt } f = \text{wt } g = 1$, we have $\text{wt } h = 1$ by (ii); and then $h(x) \in \mathbb{Z}[x]$ by (i). By comparing leading terms, $h(x)$ is also monic. \square

In the light of Theorem A1.2, it is useful to have tests for irreducibility of polynomials. In the case of number fields, the most useful such test is the following.

Theorem A2.3. Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$ iff it is irreducible in $\mathbb{Z}[x]$.

Proof. Any nontrivial factorization $f(x) = f_1(x)f_2(x)$, with nonconstant factors $f_i(x) \in \mathbb{Z}[x]$, gives a nontrivial factorization in $\mathbb{Q}[x]$. For the converse, let $f(x) \in \mathbb{Z}[x]$ and suppose that $f(x)$ is reducible in $\mathbb{Q}[x]$. We may assume $\text{wt } f(x) = 1$; otherwise divide $f(x)$ by its weight. By assumption, $f(x) = f_1(x)f_2(x)$ where each of the factors $f_i(x) \in \mathbb{Q}[x]$ has degree at least 1. Now $f_i(x) = r_i u_i(x)$ where $r_i = \text{wt } f_i(x)$ and $u_i(x) \in \mathbb{Z}[x]$. By Lemma A2.1, $\text{wt}(u_1(x)u_2(x)) = \text{wt}(u_1(x))\text{wt}(u_2(x)) = 1$, so $f(x) = u_1(x)u_2(x)$ where each of the factors $u_i(x) \in \mathbb{Z}[x]$ has degree at least 1. \square

The following criterion is more specialized but sometimes useful.

Theorem A2.4 (Eisenstein's Criterion). Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ where a_0, a_1, \dots, a_n are all divisible by some prime p which does not divide a_n . Suppose further that p^2 does not divide a_0 . Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and hence also in $\mathbb{Q}[x]$).

Proof. Supposing that $f(x)$ is reducible in $\mathbb{Z}[x]$, then $f(x) = g(x)h(x)$ where $g(x) \in \mathbb{Z}[x]$ has leading term bx^k , $h(x) \in \mathbb{Z}[x]$ has leading term cx^{n-k} with $1 \leq k \leq n-1$; and $bc = a_n$ which is not divisible by p . Reducing mod p gives a factorization of $a_nx^n \pmod{p}$ in $\mathbb{F}_p[x]$. Since \mathbb{F}_p is a field, $\mathbb{F}_p[x]$ has unique factorization; and so after reduction mod p , $g(x)$ and $h(x)$ must reduce to bx^k and $cx^{n-k} \pmod{p}$ respectively. This means that the original polynomials $g(x), h(x) \in \mathbb{Z}[x]$ must both have constant term divisible by p . But this means that $f(x) = g(x)h(x)$ must have constant term divisible by p^2 , a contradiction. \square

Appendix A3: Algebraic Integers

We recommend [Sa] for further details on algebraic integers.

A complex number $\theta \in \mathbb{C}$ is **algebraic** if it is algebraic over \mathbb{Q} , i.e. if it is a root of some nonzero polynomial $f(x) \in \mathbb{Q}[x]$. Without loss of generality, $f(x) \in \mathbb{Z}[x]$; otherwise multiply $f(x)$ by the least common denominator of its coefficients. But the resulting polynomial $f(x) \in \mathbb{Z}[x]$ is not necessarily monic.

Theorem A3.1. Let $\theta \in \mathbb{C}$ be algebraic, and let $m(x) \in \mathbb{Q}[x]$ be its minimal polynomial. Then the following conditions are equivalent.

- (i) $m(x) \in \mathbb{Z}[x]$.
- (ii) θ is a root of some monic polynomial with integer coefficients.
- (iii) $\mathbb{Z}[\theta]$ is a finitely generated as an additive group (or \mathbb{Z} -submodule of \mathbb{C}).
- (iv) There is a chain of subrings $\mathbb{Z}[\theta] \subseteq R \subset \mathbb{C}$ such that R is a finitely generated as an additive group (or \mathbb{Z} -submodule of \mathbb{C}).

Proof. We will prove (i) \Leftrightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (ii). Obviously (i) implies (ii). Conversely, suppose $f(\theta) = 0$ where $f(x) \in \mathbb{Z}[x]$ is monic, and observe that $f(x) = m(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$. As in Appendix A2, let $r = \text{wt } m(x)$ and $s = \text{wt } h(x)$ so that

$$m(x) = ru_m(x), \quad h(x) = su_h(x)$$

where $u_m(x), u_h(x) \in \mathbb{Z}[x]$ have weight 1. Since $f(x) \in \mathbb{Z}[x]$ is monic, $\text{wt } f(x) = 1$. By Lemma A2.1, $rs = 1$ so

$$f(x) = ru_m(x)su_h(x) = u_m(x)u_h(x).$$

Since $u_m(x) = \frac{1}{r}m(x)$ has positive leading term $\frac{1}{r}$, comparing leading coefficients on the left and right (these being integers) gives $r = s = 1$. In particular, $m(x) = u_m(x) \in \mathbb{Z}[x]$. This gives (i).

Now suppose (ii) holds. There exist $n \geq 0$ and integers $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$ such that

$$\theta^n + a_{n-1}\theta^{n-1} + \dots + a_1\theta + a_0 = 0.$$

In this case, the elements $1, \theta, \theta^2, \dots, \theta^{n-1}$ generate $\mathbb{Z}[\theta]$ as an additive group. To see this, note that the additive subgroup generated by $1, \theta, \dots, \theta^{n-1}$ is

$$A := \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 + \dots + \mathbb{Z}\theta^{n-1} \subseteq \mathbb{Z}[\theta].$$

Our hypothesis shows that $\theta^n \in A$. Multiplying both sides by θ yields $\theta^{n+1} \in A$. Proceeding inductively, $\theta^j \in A$ for all $j \geq 0$, and so $A = \mathbb{Z}[\theta]$, which gives (iii).

It is obvious that (iii) implies (iv). Finally suppose (iv) holds, and let $\alpha_1, \alpha_2, \dots, \alpha_n \in R$ such that

$$R = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n.$$

Denote by $T : R \rightarrow R$ the \mathbb{Z} -module homomorphism (i.e. homomorphism of additive groups) defined by $\alpha \mapsto \theta\alpha$. There exist $a_{ij} \in \mathbb{Z}$ such that

$$T(\alpha_i) = \theta\alpha_i = \sum_{j=1}^n a_{ij}\alpha_j.$$

(In general the choice of coefficients $a_{ij} \in \mathbb{Z}$ is not unique; however, this point does not affect our argument.) Then $f(T) = 0$ where $f(x) = \det(xI - A)$, $A = [a_{ij} : 1 \leq i, j \leq n]$. Clearly $f(T) : R \rightarrow R$ is the \mathbb{Z} -module homomorphism (i.e. homomorphism of additive groups) $\alpha \mapsto f(\theta)\alpha = f(T)\alpha = 0$. Since R has no zero divisors, this implies that $f(\theta) = 0$. But $f(x) \in \mathbb{Z}[x]$ is monic by construction, so (ii) follows. \square

A number $\theta \in \mathbb{C}$ is **integral** (and θ is an **algebraic integer**, or simply an **integer**) if the equivalent conditions of Theorem A3.1 hold. We denote by \mathbb{I} the set of all algebraic integers, also called the **ring of algebraic integers**, as justified by part (i) of the following. To distinguish the ‘ordinary’ integers, elements of \mathbb{Z} are called **rational integers**, and this terminology is justified by part (ii) of the following.

Theorem A3.2. (i) If $\alpha, \beta \in \mathbb{I}$ then $\alpha \pm \beta, \alpha\beta \in \mathbb{I}$. Thus $\mathbb{I} \subset \mathbb{A}$ is a subring.
 (ii) The algebraic integers in \mathbb{Q} are exactly the elements of \mathbb{Z} . That is, $\mathbb{I} \cap \mathbb{Q} = \mathbb{Z}$.
 (iii) Every element $\theta \in \mathbb{A}$ satisfies $k\theta \in \mathbb{I}$ for some positive integer k . In particular, \mathbb{A} is the field of quotients of \mathbb{I} ; and the abelian group quotient \mathbb{A}/\mathbb{I} is an infinite torsion group (i.e. every element has finite order).

Proof. (i) Let m and n be the degrees of α and β over \mathbb{Q} , respectively. Then $\mathbb{Z}[\alpha, \beta] = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \mathbb{Z}\alpha^i\beta^j$. Since $\mathbb{Z}[\alpha+\beta] \subseteq \mathbb{Z}[\alpha, \beta]$ where $\mathbb{Z}[\alpha, \beta]$ is finitely generated, $\alpha+\beta \in \mathbb{I}$ by Theorem A3.1. The same argument holds for $\alpha-\beta$ and $\alpha\beta$.

(ii) The minimal polynomial of $r \in \mathbb{Q}$ over \mathbb{Q} is $m(x) = x - r$. Use the characterization of algebraic integers given in Theorem A3.1(i).

(iii) Let $\theta \in \mathbb{A}$ be a root of $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Q}[x]$. Choose $k \in \mathbb{Z}$ such that $ka_i \in \mathbb{Z}$ for all i . Then $\alpha = k\theta$ is a root of

$$k^n m\left(\frac{x}{k}\right) = x^n + ka_{n-1}x^{n-1} + k^2a_{n-2}x^{n-2} + \cdots + k^{n-1}a_1x + k^na_0 \in \mathbb{Z}[x]$$

so that $\alpha \in \mathbb{I}$. \square

A **number field** is a finite extension field $E \supseteq \mathbb{Q}$. The **ring of integers** of E is the subring $\mathcal{O} = \mathcal{O}_E = \mathbb{I} \cap E$. An argument similar to the above shows that E is the quotient field of \mathcal{O} . The following is extremely useful in determining the ring of integers \mathcal{O}_E in an extension $E \supseteq \mathbb{Q}$, as the subsequent examples show.

Theorem A3.3. Let $E \supseteq \mathbb{Q}$ be a number field, and let $\alpha \in \mathcal{O}_E$. Denote by $T_\alpha : E \rightarrow E$ the \mathbb{Q} -linear transformation $u \mapsto \alpha u$. Then the characteristic polynomial of T_α is the monic polynomial $\det(xI - T_\alpha) = h(x)^{[E:\mathbb{Q}[\alpha]]} \in \mathbb{Z}[x]$ where $h(x)$ is the minimal polynomial of α over \mathbb{Q} . In particular, $\text{Tr}_{E/\mathbb{Q}} \alpha = \text{tr } T_\alpha \in \mathbb{Z}$ and $N_{E/\mathbb{Q}} \alpha = \det T_\alpha \in \mathbb{Z}$.

Proof. We may use $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ as a basis for $F = \mathbb{Q}[\alpha]$, and let $\{\beta_1, \beta_2, \dots, \beta_m\}$ be a basis for E over F ; thus $m = [F : \mathbb{Q}]$ and $mn = [E : \mathbb{Q}]$ (see the proof of Theorem A1.1). The matrix of $T = T_\alpha$ with respect to the basis $\{\alpha^j \beta_i : 1 \leq i \leq m, 1 \leq j \leq n\}$ is $I_m \otimes M$ where M is the $n \times n$ companion matrix of $h(x)$. The result follows. \square

Theorem A3.4. Let $E \supseteq \mathbb{Q}$ be an extension of degree n . Then E has an F -basis $\{\theta_1, \dots, \theta_n\}$ consisting of algebraic integers, such that $\{\theta_1, \dots, \theta_n\}$ is also a base for \mathcal{O}_E over \mathbb{Z} , i.e.

$$\mathcal{O}_E = \mathbb{Z}\theta_1 + \mathbb{Z}\theta_2 + \cdots + \mathbb{Z}\theta_n.$$

In other words, \mathcal{O}_E is a free \mathbb{Z} -module of rank $n = [E : \mathbb{Q}]$.

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for E over \mathbb{Q} . Without loss of generality, each $\alpha_i \in \mathcal{O}$; otherwise, by Theorem A3.2(iii), replace α_i by a positive integer multiple thereof. Consider the free abelian group (i.e. \mathbb{Z} -submodule of E) generated by our basis:

$$L = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n \subseteq \mathcal{O}.$$

Using the nondegenerate bilinear form in Theorem A1.6, there is another basis $\{\beta_1, \dots, \beta_n\}$ of E over \mathbb{Q} , dual to the first basis, such that $\text{Tr}_{E/\mathbb{Q}}(\alpha_i \beta_j) = \delta_{ij}$. Now given $\theta \in \mathcal{O}$, we may express θ as a linear combination of the second basis as $\theta = \sum_{j=1}^n b_j \beta_j$ for some $b_j \in \mathbb{Q}$. Since $\alpha_i, \theta \in \mathcal{O}$ for each i , we have $\alpha_i \theta \in \mathcal{O}$ and so $b_i = \text{Tr}_{E/\mathbb{Q}}(\alpha_i \theta) \in \mathbb{Z}$. This shows that

$$\mathcal{O} \subseteq \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \cdots + \mathbb{Z}\beta_n,$$

so \mathcal{O} is a free abelian group of rank at most n . Recalling that \mathcal{O} has a subgroup L which is free abelian of rank exactly n , this forces \mathcal{O} to be free abelian also of rank n . \square

Now let $E \supseteq \mathbb{Q}$ be an extension of degree n , with ring of integers \mathcal{O} . By Theorem A3.4, there is a basis $\{\theta_1, \dots, \theta_n\}$ for E over \mathbb{Q} which also generates \mathcal{O} as a \mathbb{Z} -module. Define the **discriminant** of the extension $E \supseteq \mathbb{Q}$ to be

$$\text{disc}(\theta_1, \dots, \theta_n) = \det[\text{Tr}_{E/\mathbb{Q}}(\theta_i \theta_j) : 1 \leq i, j \leq n].$$

This determinant is a *nonzero* integer since it is the Gram matrix of our nondegenerate bilinear form $[a, b] = \text{Tr}_{E/\mathbb{Q}}(ab)$ with respect to our base. Now consider another base $\{\theta'_1, \dots, \theta'_n\}$ for \mathcal{O} over \mathbb{Z} , so that $\theta'_i = \sum_{j=1}^n a_{ij} \theta_j$ and the matrix $A = [a_{ij} : 1 \leq i, j \leq n]$ has integer entries. The inverse matrix A^{-1} expressing the original base of θ_i 's in terms of the θ'_j 's must similarly have integer entries; and so $\det A = \pm 1$. then

$$\begin{aligned} \text{disc}(\theta'_1, \dots, \theta'_n) &= \det[\text{Tr}_{E/\mathbb{Q}}(\theta'_i \theta'_j) : 1 \leq i, j \leq n] = \det(A)^2 \text{disc}(\theta_1, \dots, \theta_n) \\ &= \text{disc}(\theta_1, \dots, \theta_n). \end{aligned}$$

So the discriminant of a finite extension over \mathbb{Q} is well-defined, independent of the choice of base. (For more general finite extensions $E \supseteq F$, however, the discriminant is well-defined only up to multiplication by the square of a unit.)

Example A3.5: Quadratic Fields. Consider a quadratic extension $E = \mathbb{Q}[\sqrt{d}] \supset \mathbb{Q}$ where $d \neq 1$ is a squarefree integer (i.e. a product of distinct primes). The extension is **real quadratic** if $d \geq 2$; or **imaginary quadratic** if $d \leq -1$. The matrix of T_α , $\alpha = a + b\sqrt{d} \in \mathcal{O}_E$ with respect to the basis $\{1, \sqrt{d}\}$ is $\begin{bmatrix} a & db \\ b & a \end{bmatrix}$. In order that $\alpha \in \mathcal{O}_E$, Theorem A3.4 requires that both $\text{Tr}_{E/\mathbb{Q}} \alpha = 2a$ and $N_{E/\mathbb{Q}} \alpha = a^2 - db^2$ are integers. We have two cases. (Note that $d \not\equiv 0 \pmod{4}$ since d is naturally assumed to be squarefree.)

(i) When $d \equiv 2$ or $3 \pmod{4}$, this simplifies to $a, b \in \mathbb{Z}$ and we have $\mathcal{O} \subseteq \mathbb{Z}[\sqrt{d}]$; and the reverse containment is clear, so $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ has base $\{1, \sqrt{d}\}$. The discriminant is $D := \det \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d$.

(ii) When $d \equiv 1 \pmod{4}$, we instead have $a = \frac{u}{2}$ and $b = \frac{v}{2}$ where $u, v \in \mathbb{Z}$ with $u \equiv v \pmod{2}$ so $\mathcal{O} \subseteq \mathbb{Z}[\theta]$ where $\theta = \frac{1}{2}(1 + \sqrt{d})$, and once again equality holds: $\mathcal{O} = \mathbb{Z}[\theta]$ has base $\{1, \theta\}$. In this case the discriminant is $D = \det \begin{bmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{bmatrix} = d$.

As above, let E be a number field, and \mathcal{O} its ring of integers. Denote by \mathcal{O}^\times the group of **units** (invertible elements) in \mathcal{O} . By abuse of language, these are often called the units of E . In the following, r denotes the number of embeddings of E in \mathbb{R} (i.e. ring monomorphisms $E \rightarrow \mathbb{R}$) and $2s$ is the number of pairs (under complex conjugation) of embeddings $E \rightarrow \mathbb{C}$ which do not lie in \mathbb{R} . The total number of embeddings of E in \mathbb{C} is $r + 2s = [E : \mathbb{Q}]$. (This relation, and the following theorem, hold for any finite extension $E \supseteq \mathbb{Q}$, Galois or not.)

Theorem A3.6 (Dirichlet). A maximal free subgroup $G < \mathcal{O}^\times$ has rank $r + s - 1$. Every unit $\alpha \in \mathcal{O}^\times$ is uniquely factorizable as $\alpha = \zeta g$ where ζ is a root of unity, and $g \in G$. Thus $\mathcal{O}^\times = U \times G$ where U is finite cyclic and $G \cong \mathbb{Z}^{r+s-1}$.

Proof. See [Sa, p.60]. □

Example A3.7: The Rationals. \mathbb{Q} has $(r, s) = (1, 0)$ and all its units $\mathbb{Z}^\times = \{\pm 1\}$ are roots of unity, a cyclic group of order 2.

Example A3.8: An Imaginary Quadratic Field. The imaginary quadratic extension $E = \mathbb{Q}[\sqrt{-3}] \supset \mathbb{Q}$ has $(r, s) = (0, 1)$. Its ring of integers $\mathcal{O} = \mathbb{Z}[\omega]$, $\omega = \zeta_3 = \frac{1}{2}(1 + \sqrt{-3})$ has a group of units $\mathcal{O}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ which is cyclic of order 6. There are no units of infinite order, as $r + s - 1 = 0$. As explained above, $\{1, \omega\}$ is a base for \mathcal{O} . For $\alpha = a + b\omega$ we have $T_\alpha = \begin{bmatrix} a & -b \\ b & a-b \end{bmatrix}$ with respect to our base; and $N_{E/\mathbb{Q}}\alpha = a^2 - ab + b^2$. To find units, we require integer solutions of $N_{E/\mathbb{Q}}(a+b\omega) = a^2 - ab + b^2 = \frac{3}{4}a^2 + \frac{1}{4}(a-2b)^2 = 1$. The equation requires $|a| \leq 1$, and a similar argument gives $|b| \leq 1$. After checking all nine pairs (a, b) satisfying these inequalities, we find only six solutions of the Diophantine equation, viz. $(a, b) \in \{\pm(1, 0), \pm(0, 1), \pm(1, 1)\}$ which gives the six units listed above.

Example A3.9: A Real Quadratic Field. The real quadratic extension $E = \mathbb{Q}[\sqrt{7}] \supset \mathbb{Q}$ has $(r, s) = (2, 0)$. Its ring of integers $\mathcal{O} = \mathbb{Z}[\sqrt{7}]$ has units $\mathcal{O}^\times = \{\pm g^k : k \in \mathbb{Z}\}$ including two roots of unity ± 1 and the unit $g = 8 + 3\sqrt{7}$ which generates an infinite cyclic group (a free group on $r + s - 1 = 1$ generator). The norm map $N = N_{E/\mathbb{Q}} : \mathcal{O} \rightarrow \mathbb{Z}$, $a + b\sqrt{7} \mapsto a^2 - 7b^2$ is similarly useful in verifying these claims; but we omit the details.

Two nonzero elements $\alpha, \beta \in \mathcal{O}$ generate the same principal ideal, i.e. $\alpha\mathcal{O} = \beta\mathcal{O}$, iff $\beta = u\alpha$ for some $u \in \mathcal{O}^\times$. In this case we say α and β are **associates** in \mathcal{O} . Denote by S_E the set of all nonzero elements of \mathcal{O}_E which are not units. An element $\alpha \in S_E$ is **reducible** if $\alpha = \beta\gamma$ for some $\beta, \gamma \in S_E$. If α is not reducible, it is **irreducible** (in \mathcal{O}). Assuming $\alpha, \alpha' \in S_E$ are associates, then α is reducible iff α' is. Every element in S_E is expressible as a finite product of irreducible elements; but this factorization is not in general unique since any factorization $\alpha = \pi_1\pi_2 \cdots \pi_k$ (with irreducible factors π_1, \dots, π_k) yields other such factorizations through permutations of the k factors, or through the replacement of the irreducible factors by suitable associates (a process called **migration of units**). We say \mathcal{O}_E (or, abusing language, E itself) has **unique factorization**, if every element $\alpha \in S_E$ factors into irreducible factors in an essentially unique way (i.e. up to permutation of the factors, and migration of units). Not every ring of integers \mathcal{O}_E has unique factorization (i.e. of elements). But \mathcal{O}_E always has unique factorization of ideals (Theorem A3.10 below). When \mathcal{O} is a principal ideal ring, this forces elements to also have unique factorization; but since ideals in \mathcal{O} are not necessarily principal, we do not always obtain unique factorization of elements.

It might help here to keep in mind the hierarchy $\text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{ID}$ where an **integral domain (ID)** is a commutative ring with identity having no zero divisors; a **unique factorization domain (UFD)** is an integral domain with unique factorization (of elements as product of irreducibles); a **principal ideal domain (PID)** is an integral domain in which every ideal is principal; and a **Euclidean domain (ED)** is an integral domain in which the ‘division algorithm’ holds. More about this appears at the end of this Appendix. Since our interest focuses on the special case of the ring \mathcal{O} of integers

in a number field, the hierarchy simplifies (see Theorem A3.14). In particular the rule $\text{PID} \Rightarrow \text{UFD}$ has a valid converse in the case of rings of integers, but not in the general case; recall that $\mathbb{Z}[x]$ is a UFD with a nonprincipal ideal $(2, x)$. We will postpone the relevant theorem until after presenting some examples of rings of integers in a few specific number fields. And before that, we need to review some terminology.

Recall that an **ideal** is an additive subgroup $\mathcal{A} \subseteq \mathcal{O}$ such that $\mathcal{O}\mathcal{A} \subseteq \mathcal{A}$, i.e. $ra \in \mathcal{A}$ for all $r \in \mathcal{O}$, $a \in \mathcal{A}$. The **sum** and **product** of two ideals are the ideals defined by

$$\begin{aligned} \mathcal{A} + \mathcal{B} &= \{a + b : a \in \mathcal{A}, b \in \mathcal{B}\}; \\ \mathcal{A}\mathcal{B} &= \{\text{finite sums of products } ab \text{ with } a \in \mathcal{A}, b \in \mathcal{B}\} \\ &= \{a_1b_1 + a_2b_2 + \cdots + a_kb_k : k \geq 1, a_1, a_2, \dots, a_k \in \mathcal{A}, b_1, b_2, \dots, b_k \in \mathcal{B}\}. \end{aligned}$$

We often abbreviate $(a) = a\mathcal{O} \subseteq \mathcal{O}$ for the **principal ideal** generated by an element $a \in \mathcal{O}$. More generally, the ideal generated by a list of elements $a_1, \dots, a_k \in \mathcal{O}$ is

$$(a_1, a_2, \dots, a_k) := (a_1) + (a_2) + \cdots + (a_k) = \mathcal{O}a_1 + \mathcal{O}a_2 + \cdots + \mathcal{O}a_k \subseteq \mathcal{O}.$$

Two elements $a, b \in \mathcal{O}$ generate the same ideal $(a) = (b)$ iff a and b are associates. A proper ideal $\mathfrak{P} \subset \mathcal{O}$ is **prime** any of the following equivalent conditions are satisfied:

- (i) Whenever $ab \in \mathfrak{P}$ with $a, b \in \mathcal{O}$, we must have $a \in \mathfrak{P}$ or $b \in \mathfrak{P}$.
- (ii) If $\mathfrak{P} \subseteq \mathcal{A}\mathcal{B}$ where $\mathcal{A}, \mathcal{B} \subseteq \mathcal{O}$ are ideals, we have $\mathfrak{P} \subseteq \mathcal{A}$ or $\mathfrak{P} \subseteq \mathcal{B}$.
- (iii) The quotient ring \mathcal{O}/\mathfrak{P} is an integral domain (i.e. it has no zero divisors).

A nonzero principal ideal $(\pi) \subset \mathcal{O}$ is prime iff its generator π is irreducible. A proper ideal $\mathcal{M} \subset \mathcal{O}$ is **maximal** if there is no proper ideal of \mathcal{O} which strictly contains \mathcal{M} ; equivalently, \mathcal{O}/\mathcal{M} is a field. So every maximal ideal is prime. The converse is not true in general, but the ring of integers \mathcal{O} of a number field is special in many ways including this:

Theorem A3.10. Let $E \supseteq \mathbb{Q}$ be a finite extension with ring of integers $\mathcal{O} = \mathcal{O}_E$.

- (i) The **norm** of an ideal $\mathcal{A} \subseteq \mathcal{O}$, defined as its index $N(\mathcal{A}) := |\mathcal{O}/\mathcal{A}|$, is a positive integer whenever $\mathcal{A} \neq (0)$. The norm map is multiplicative: $N(\mathcal{A}\mathcal{B}) = N(\mathcal{A})N(\mathcal{B})$ for any two ideals $\mathcal{A}, \mathcal{B} \subseteq \mathcal{O}$. The unique ideal of norm 1 is the ring \mathcal{O} itself. The norm of its principal ideal is the (absolute value of the) norm of its generator: $N((a)) = |N_{E/\mathbb{Q}}(a)|$ for all nonzero $a \in \mathcal{O}$.
- (ii) Every nonzero prime ideal of \mathcal{O} is maximal. There is a unique rational prime $p \in \mathfrak{P} \cap \mathbb{Z}$, and the quotient ring \mathcal{O}/\mathfrak{P} is a finite field of order $q = p^f$ where $f \geq 1$.
- (iii) Every nonzero ideal $\mathcal{A} \subseteq \mathcal{O}$ factors as a product $\mathcal{A} = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_k$ for some (not necessarily distinct) prime ideals $\mathfrak{P}_i \subset \mathcal{O}$. (An empty product of ideals is simply \mathcal{O} .) This factorization is unique up to permutation of the prime factors.
- (iv) For each rational prime p , the ideal $(p) = p\mathcal{O}$ has prime factorization $(p) = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_d^{e_d}$ where the prime factors $\mathfrak{P}_i \subset \mathcal{O}$ are distinct; $e_i \geq 1$; $N(\mathfrak{P}_i) = p^{f_i}$; and $e_1f_1 + \cdots + e_df_d = [E : \mathbb{Q}]$.

In (iv), each quotient field $\mathcal{O}/\mathfrak{P}_i$ is a **residual field**; the degree f_i of its extension over \mathbb{F}_p is the **residual degree**; and the number of times e_i that \mathfrak{P}_i divides (p) is the **ramification index** of \mathfrak{P}_i . We say p **ramifies** in E if at least one of the indices satisfies $e_i > 1$. We say p **remains prime** if $(p) = p\mathcal{O} \subset \mathcal{O}$ is prime; and p **splits** if there are $d \geq 2$ distinct prime factors. There are only finitely many primes which ramify (namely, those primes which divide the discriminant). For Galois extensions, (iv) simplifies to $(p) = (\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_d)^e$, i.e. all ramification indices coincide: $e_i = e$.

Example A3.11: The Rational Integers. \mathbb{Z} has unique factorization. Here the irreducible elements have the form $\pm p$ where p is an ordinary prime (of course p and $-p$ are associates) and the corresponding prime ideals have the form $(p) = p\mathbb{Z}$. All ideals are principal, and unique factorization of elements is due to unique factorization of ideals; for example, $(12) = (2)^2(3)$ yields $12 = 2^2 \cdot 3$. Addition of ideals corresponds to taking greatest common divisors: $(a_1) + (a_2) + \cdots + (a_k) = (a_1, a_2, \dots, a_k) = (d)$ where $d = \gcd(a_1, a_2, \dots, a_k)$.

Example A3.12: An Imaginary Quadratic Extension. The imaginary quadratic extension $E = \mathbb{Q}[\theta]$, $\theta = \sqrt{-6}$, does not have unique factorization. Its ring of integers is $\mathcal{O} = \mathbb{Z}[\theta]$ and its units are $\mathcal{O}^\times = \{\pm 1\}$. The element 6 factors in two essentially different ways as $6 = 2 \cdot 3 = (-\theta)\theta$, where the indicated factors are irreducible. These properties are easily verified using the norm map $N = N_{E/\mathbb{Q}} : \mathcal{O} \rightarrow \mathbb{Z}$, $a + b\theta \mapsto a^2 + 6b^2$ using the identity $N(\alpha\beta) = N(\alpha)N(\beta)$. If $\alpha\beta = 1$ in \mathcal{O} , then $N(\alpha)N(\beta) = 1$. Since norms of elements in \mathcal{O} are nonnegative integers, this forces $N(\alpha) = N(\beta) = 1$; and since the equation $a^2 + 6b^2 = 1$ yields $(a, b) = (\pm 1, 0)$ as its only integer solutions, we obtain $\mathcal{O}^\times = \{\pm 1\}$. Supposing $2 = \alpha\beta$ where $\alpha, \beta \in \mathcal{O}$, then $N(\alpha)N(\beta) = N(2) = 4$. Clearly the equation $a^2 + 6b^2 = 2$ has no integer solutions; so one of the factors α, β has norm one and thus is a unit. This proves that 2 is irreducible in \mathcal{O} ; and a similar argument shows that 3 and $\pm\theta$ are irreducible in \mathcal{O} . Finally, since the only units are ± 1 , it is easy to see that our two factorizations of 6 in \mathcal{O} are essentially different.

The ideal $(6) \subset \mathcal{O}$ has norm 36, and its prime factorization is $(36) = \mathfrak{P}^2\mathfrak{Q}^2$ where the prime ideals $\mathfrak{P} = (2, \theta)$ and $\mathfrak{Q} = (3, \theta)$ have norm 2 and 3 respectively. Here $(2) = \mathfrak{P}^2$ has norm 4, $(3) = \mathfrak{Q}^2$ has norm 9, and $(\theta) = \mathfrak{P}\mathfrak{Q}$ has norm 6. The extension has discriminant $D = -36$ (see Example A3.5(i)); and the primes 2 and 3 are the only primes that ramify (each with ramification index 2).

The rational prime 13 remains prime since $\mathcal{O}/(13) \cong \mathbb{Z}[x]/(13, x^2+6) \cong \mathbb{F}_{13}[x]/(x^2+6) \cong \mathbb{F}_{169}$. Here we use the fact that -6 is a nonsquare mod 13, i.e. $(\frac{-6}{13}) = -1$. By quadratic reciprocity, all rational primes congruent to 13, 17, 19 or 23 mod 24 similarly remain prime in E .

The rational prime 11 splits as $(11) = \mathfrak{P}_{11}\overline{\mathfrak{P}}_{11}$ where $\mathfrak{P}_{11} = (11, 4+\theta)$ and $\overline{\mathfrak{P}}_{11} = (11, 7+\theta)$. This follows from $\mathcal{O}/11\mathcal{O} \cong \mathbb{Z}[x]/(11, x^2+6) \cong \mathbb{F}_{11}[x]/(x^2+6) \cong \mathbb{F}_{11}[x]/(x-4) \oplus \mathbb{F}_{11}[x]/(x-7) \cong \mathbb{F}_{11} \oplus \mathbb{F}_{11}$. By quadratic reciprocity, all primes congruent to 1, 5, 7 or 11 mod 24 split in this way.

Example A3.13: A Quartic Extension. Let $E = \mathbb{Q}[\theta]$ where θ is a root of $f(x) = x^4 - x + 3$. Since $f(x)$ is irreducible over \mathbb{F}_2 , it is irreducible over \mathbb{Z} and hence over \mathbb{Q} . It may be shown that $\mathcal{O} = \mathbb{Z}[\theta]$ and that the quartic extension $E \supset \mathbb{Q}$ has discriminant $6885 = 3^4 \cdot 5 \cdot 17$; and the only roots of unity in \mathcal{O} are ± 1 . Since $r+s-1 = 0+2-1 = 1$ in Theorem A3.6, the unit group has the form $\mathcal{O}^\times = \{\pm g^k : k \in \mathbb{Z}\}$ for some g . Computation shows that we may take $g = \theta^2 + 2\theta + 2$, $g^{-1} = -\theta^3 + \theta^2 - 1$.

The rational prime 2 remains prime in E since $\mathcal{O}/2\mathcal{O} \cong \mathbb{Z}[x]/(2, f(x)) \cong \mathbb{F}_2[x]/(x^4+x+1) \cong \mathbb{F}_{16}$ (Example 3.3). Its residual degree is 4. Similarly, 11, 13, 43, 53, 61, ... remain prime.

The rational prime 3 ramifies as $(3) = \mathfrak{P}_{3a}\mathfrak{P}_{3b}^3$ where both distinct factors $\mathfrak{P}_{3a} = (3, \theta)$ and $\mathfrak{P}_{3b} = (3, 2+\theta)$ have residual degree 1. This follows from $\mathcal{O}/3\mathcal{O} \cong \mathbb{Z}[x]/(3, f(x)) \cong \mathbb{F}_3[x]/(x(x+2)^3) \cong \mathbb{F}_3[x]/(x) \oplus \mathbb{F}_3[x]/((x+2)^3) \cong \mathbb{F}_3 \oplus S$ where $S \cong \mathbb{F}_3[x]/(x^3)$ is a local ring of order 27. Although the residual degrees coincide ($f_1 = f_2 = 1$), the ramification indices $e_1 = 1$ and $e_2 = 3$ do not. This points to the fact that the extension is not Galois.

The rational prime 17 ramifies as $(17) = \mathfrak{P}_{17}^2\mathfrak{P}'_{17}\mathfrak{P}''_{17}$ where $\mathfrak{P}_{17} = (17, 13+\theta)$, $\mathfrak{P}'_{17} = (17, 10+\theta)$, $\mathfrak{P}''_{17} = (17, 15+\theta)$. Here $\mathcal{O}/17\mathcal{O} \cong \mathbb{Z}[x]/(17, f(x)) \cong \mathbb{F}_{17}[x]/((x+13)^2(x+10)(x+15)) \cong R \oplus \mathbb{F}_{17} \oplus \mathbb{F}_{17}$ where $R = \mathbb{F}_{17}[\varepsilon]/(\varepsilon^2)$ is the ring of **dual numbers** over \mathbb{F}_{17} , a local ring of order 289. Again the ramification indices 2,1,1 do not all coincide.

The rational prime 5 ramifies as $(5) = \mathfrak{P}_5^2\mathfrak{P}'_5$ where the distinct prime ideals $\mathfrak{P}_5 = (5, 1+\theta)$ and $\mathfrak{P}'_5 = (5, 3+3\theta+\theta^2)$ have residual degrees 1,2 and ramification indices 2,1. Here $\mathcal{O}/5\mathcal{O} \cong \mathbb{Z}[x]/(5, f(x)) \cong \mathbb{F}_5[x]/((x+1)^2(x^2+3x+3)) \cong R \oplus \mathbb{F}_{25}$ where R is the ring of dual numbers over \mathbb{F}_5 .

The rational prime 7 splits as $(7) = \mathfrak{P}_7\mathfrak{P}'_7$ where the residual degrees are 1,3 and both ramification indices are 1. Here $\mathcal{O}/7\mathcal{O} \cong \mathbb{Z}[x]/(7, f(x)) \cong \mathbb{F}_7[x]/((x+2)(x^3+5x^2+4x+5)) \cong \mathbb{F}_7 \oplus \mathbb{F}_{343}$. We find a similar behaviour at the primes 19, 23, 37, 59, ...

The rational prime 29 splits as $(29) = \mathfrak{P}_{29}\mathfrak{P}'_{29}\mathfrak{P}''_{29}$ with residual degrees 1,1,2 and ramification indices 1,1,1. Here $\mathcal{O}/29\mathcal{O} \cong \mathbb{Z}[x]/(29, f(x)) \cong \mathbb{F}_{29}[x]/((x+3)(x+6)(x^2+20x+5)) \cong \mathbb{F}_{29} \oplus \mathbb{F}_{29} \oplus \mathbb{F}_{841}$. We find a similar behaviour at the primes 31, 41, 47, ...

The examples above illustrate, among other things, the existence of nonprincipal ideals in exactly those cases where unique factorization (of elements) fails. This is no coincidence:

Theorem A3.14. Let \mathcal{O} be the ring of integers \mathcal{O} in a number field. Then \mathcal{O} is a unique factorization domain if and only if \mathcal{O} is a principal ideal domain.

As we have previously reminded the reader, for general integral domains, the PID property does not imply the UFD property; an example is the ring $\mathbb{Z}[x]$ which is a UFD but the ideal $(2, x)$ is nonprincipal.

Proof of Theorem A3.14. Suppose \mathcal{O} is a principal ideal domain, and suppose $a, b \in \mathcal{O}$ such that ab is divisible by an irreducible element p . Since $ab = pd$ for some $d \in \mathcal{O}$, $(a)(b) = (p)(d)$. But ideals in \mathcal{O} factor uniquely, and the nonzero ideal $(p) \subset \mathcal{O}$ is prime; so $(a) \subseteq (p)$ or $(b) \subseteq (p)$, i.e. p divides a or p divides b .

For the converse, let $\mathcal{A} \subseteq \mathcal{O}$ be an arbitrary ideal, and we must show that \mathcal{A} is principal. We may assume \mathcal{A} is nonzero, so $\mathcal{A} = \mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_k$ is a product of nonzero prime ideals \mathfrak{P}_i . If each \mathfrak{P}_i is principal, so is \mathcal{A} ; thus we may assume $\mathcal{A} = \mathfrak{P}$ is itself a nonzero prime ideal. Now $\mathfrak{P} \cap \mathbb{Z}$ is a prime ideal in \mathbb{Z} , so $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p . (Alternatively, \mathcal{O}/\mathfrak{P} is a finite field, so $\mathcal{O}/\mathfrak{P} \cong \mathbb{F}_q$ where $q = p^e$, $e \geq 1$ and p is prime.) Let $p = \pi_1\pi_2 \cdots \pi_r$ be the unique factorization of p as a product of irreducibles in \mathcal{O} . Since $p = \pi_1\pi_2 \cdots \pi_r \in \mathfrak{P}$ where the ideal \mathfrak{P} is prime, we have $\pi_i \in \mathfrak{P}$ for some i . Now $(\pi_i) \subseteq \mathfrak{P} \subset \mathcal{O}$; and since the nonzero prime ideal (π_i) is maximal, $(\pi_i) = \mathcal{O}$. \square

One way to verify that \mathcal{O} is a UFD (and hence a PID) is to show that it satisfies the division algorithm. We say that \mathcal{O} is **Euclidean** if for every $x, d \in \mathcal{O}$ with $d \neq 0$, there

exist $q, r \in \mathcal{O}$ such that $x = qd + r$ with $N(r) < N(d)$. More generally, any integral domain satisfying such a division algorithm is called a **Euclidean domain (ED)** (whose ‘norm’ may go by another name, such as ‘degree’, depending on the context; but we do require $N(ab) = N(a)N(b)$, $N(a) \in \{0, 1, 2, \dots\}$, and $N(a) = 0$ iff $a = 0$).

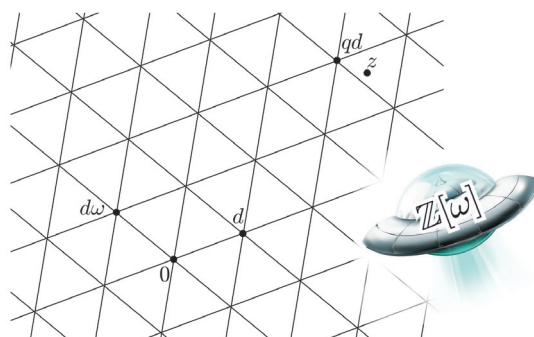
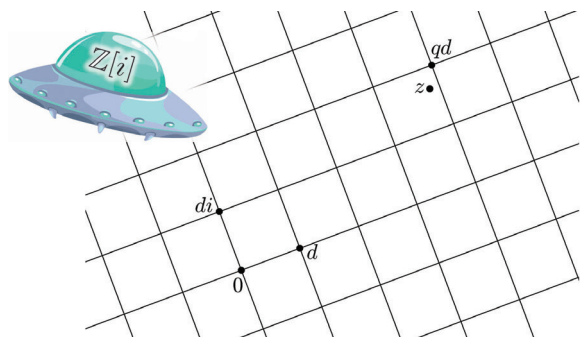
Theorem A3.15. If \mathcal{O} is a Euclidean domain, then \mathcal{O} has unique factorization (\mathcal{O} is a PID and hence also a UFD).

Proof. Let $\mathcal{A} \subseteq \mathcal{O}$. Without loss of generality, \mathcal{A} is nonzero. Choose a nonzero element $d \in \mathcal{A}$ for which $N(d)$ is as small as possible. Of course, $(d) \subseteq \mathcal{A}$. Conversely, let $a \in \mathcal{A}$. Then $a = qd + r$ where $r \in \mathcal{O}$ and $N(r) < N(d)$. However, $r = a - qd \in \mathcal{A}$; so by choice of d , we must have $r = 0$. This means that $a \in (d)$, which gives the reverse inclusion; so $\mathcal{A} = (d)$. \square

The ring of **Gaussian integers** is $\mathbb{Z}[i]$. The ring of **Eisenstein integers** is $\mathbb{Z}[\omega]$. Here $i = \zeta_4$ and $\omega = \zeta_3$.

Corollary A3.16. The rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are Euclidean. Hence these rings are UFDs, as well as PIDs.

Proof. Let $d = a + bi \in \mathbb{Z}[i]$ be nonzero. Then the principal ideal $(d) = \mathbb{Z}d + i\mathbb{Z}d \subset \mathcal{O}$ forms a square lattice (the vertices of the square grid shown, below left).



Given $z \in \mathcal{O}$, let $qd \in (d)$ be a vertex of the square grid that is closest to z . Although the choice of closest vertex may not be unique, it certainly has distance at most $\frac{|d|}{\sqrt{2}}$ from z , i.e. $N(r) = |r|^2 \leq \frac{1}{2}|d|^2 = \frac{1}{2}N(d)$ where $r = z - qd$. This shows that $\mathbb{Z}[i]$ is Euclidean. A similar argument, using a grid formed by equilateral triangles, shows that $\mathbb{Z}[\omega]$ is Euclidean. \square

Let $\mathcal{O} = \mathcal{O}_E$ be the ring of integers in a number field E (i.e. $E \supseteq \mathbb{Q}$ is a finite extension and \mathcal{O} is its ring of algebraic integers). Consider two nonzero ideals $\mathcal{A}, \mathcal{B} \subseteq \mathcal{O}$. We say \mathcal{A}

and \mathcal{B} are **equivalent** if $m\mathcal{A} = m'\mathcal{B}$ for some nonzero elements $m, m' \in \mathcal{O}$. This gives an equivalence relation on the set of nonzero ideals of \mathcal{O} . The equivalence class of \mathcal{A} , denoted by $[\mathcal{A}]$, is called the **ideal class** of \mathcal{A} . It is not hard to prove that the binary operation

$$[\mathcal{A}][\mathcal{B}] = [\mathcal{A}\mathcal{B}]$$

is well-defined for ideal classes; that is, it does not depend on the choice of representative of each ideal class. Furthermore, this operation makes the set of ideal classes of \mathcal{O} into an abelian group, called the **ideal class group** of \mathcal{O} (or of E). Since $\mathcal{O}\mathcal{A} = \mathcal{A}$, the identity element of this group is $[\mathcal{O}]$. This class consists of all the principal ideals of \mathcal{O} . Thus \mathcal{O} is a PID iff its ideal class group is trivial. Now for the *nontrivial* result:

Theorem A3.17. The ideal class group of every number field is finite.

The **class number** of a number field E , usually denoted by h_E , is the order of its ideal class group. Constructing elements of the ideal class group of a given order (if they exist) is usually not too hard; but finding explicit upper bounds on h_E is often hard. Fortunately for many of the smaller number fields of interest, class numbers and groups is within the reach of appropriate computational software.

It follows immediately that if $h = h_E$ is the class number of E , then for every ideal $\mathcal{A} \subseteq \mathcal{O}$, the ideal $\mathcal{A}^h \subseteq \mathcal{O}$ is principal. This is often an adequate substitute for having a PID. Sometimes it is helpful to note that h can be replaced here by the exponent of the ideal class group. (Recall that the **exponent** of a group is the least common multiple of the orders of the elements of that group, this being a divisor of the group order.)

Appendix A4: Normal and Separable Extensions

An algebraic extension of fields $E \supseteq F$ is **normal** if for every element $\alpha \in E$, the minimal polynomial of α over F splits into linear factors in $F[x]$. An extension $E \supseteq F$ is called a **splitting field** for a polynomial $f(x) \in F[x]$ if

- (i) $f(x)$ splits into linear factors in $E[x]$, i.e. $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where $a, \alpha_1, \dots, \alpha_n \in E$; and
- (ii) $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$; thus E is the *smallest* extension of F where $f(x)$ splits into linear factors.

Example A4.1: A Cubic Extension and its Normal Closure. Let $\theta = 2^{1/3}$ and $\omega = e^{2\pi i/3} = \frac{1}{2}(-1 + \sqrt{-3})$. The extension $L := \mathbb{Q}[\theta] \supseteq \mathbb{Q}$ is not normal since the minimal polynomial of θ over \mathbb{Q} is $m(x) = x^3 - 2 = (x - \theta)(x - \omega\theta)(x - \omega^2\theta)$, only one of whose roots lies in L . By adjoining to L the remaining roots of $f(x)$, we obtain the extension $E = \mathbb{Q}[\theta, \omega\theta, \omega^2\theta] = \mathbb{Q}[\omega, \theta] = L[\omega] \supseteq \mathbb{Q}$ which *is* normal; it is the splitting field of $m(x)$, and it is called the **normal closure** of L (the unique smallest extension of L which is normal) over \mathbb{Q} .

Theorem A4.2. (i) Let F be a field, and let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exists a splitting field $E \supseteq F$ for $f(x)$ over F ; and the splitting field is unique up to isomorphism.

(ii) A finite extension $E \supseteq F$ is normal iff it is the splitting field of some polynomial $f(x) \in F[x]$ over F .

We therefore speak of *the* splitting field (rather than *a* splitting field) for $f(x) \in F[x]$ over F . We only *sketch* the construction of the splitting field of $f(x) \in F[x]$ over F , as follows: First construct an extension $E_1 = F[\alpha_1] \cong F[x]/(f(x))$ such that $f(x) = (x - \alpha_1)g(x)$, $g(x) \in E_1[x]$, and then recursively apply this process to $g(x)$, repeating until we have obtained an extension in which $f(x)$ splits into linear factors. The resulting extension is finite by Theorem A1.1. For (ii), given a finite normal extension $E \supseteq F$, we can easily express $E = F[\alpha_1, \dots, \alpha_n]$, then take $f(x)$ to be the least common multiple (in $F[x]$) of the minimal polynomials of the generators $\alpha_1, \dots, \alpha_n$ over F ; clearly E is the splitting field of $f(x)$ over F .

An algebraic extension of fields $E \supseteq F$ is **separable** if every irreducible polynomial $f(x) \in F[x]$ has no repeated roots in E , i.e. $f(x)$ is not divisible by $(x - \alpha)^2$ for any $\alpha \in E$.

Example A4.3: An Inseparable Extension. Let $E = \mathbb{F}_p(t)$, the field of rational functions in an indeterminate t , with coefficients in the prime order field \mathbb{F}_p (thus E is the field of quotients of the polynomial ring $\mathbb{F}_p[t]$). This has a subfield $F = \mathbb{F}_p(t^p)$, and the extension $E \supset F$ has degree p with basis $\{1, t, t^2, \dots, t^{p-1}\}$. It is not separable; the polynomial $f(x) = x^p - t^p \in F[x]$ is irreducible in $F[x]$; yet it factors as $f(x) = (x-t)^p$ in $E[x]$, where it has one distinct root t with multiplicity p . Now $E = F[t] \supset F$ is the splitting field of $f(x)$, the minimal polynomial of t over F , so it is normal but inseparable. Also $\text{Tr}_{E/F} t = 0$ as seen as seen from the coefficient of x^{p-1} in $f(x)$. More generally, $\text{Tr}_{E/F}(t^k) = 0$ for $k = 0, 1, 2, \dots, p-1$ and so the trace map of the extension vanishes identically: $\text{Tr}_{E/F} = 0$. The conclusion of Theorem A1.7(ii) fails dramatically; but so does the hypothesis since E and F are infinite fields of positive characteristic p .

While examples like A4.3 do arise naturally in certain situations, throughout this course we will treat them as pathological cases to be avoided. We focus instead on fields which are either finite or have characteristic zero, which are always separable by Theorem A4.5 below.

Theorem A4.4. Let $E \supseteq K \supseteq F$ be a tower of finite fields. If the extension $E \supseteq F$ is separable, then so are the extensions $E \supseteq K$ and $K \supseteq F$.

Proof. Suppose $E \supseteq F$ is separable. Clearly $K \supseteq F$ is separable: since every $\alpha \in E$ is a simple root of its minimal polynomial over F , this is in particular true for every $\alpha \in K$. Now let $f(x) \in K[x]$ be irreducible in $K[x]$, with $f(\alpha) = 0$ for some $\alpha \in E$. Let $g(x) \in F[x]$ be the minimal polynomial of α over F . Since $f(x)$ is the minimal polynomial of α over K , $g(x) = f(x)h(x)$ for some $h(x) \in K[x]$. Since α is a simple root of $g(x)$, it is a simple root of $f(x)$. So $E \supseteq K$ is separable. \square

Theorem A4.5. Let $E \supseteq F$ be an extension of finite fields, or fields of characteristic zero. Then the extension $E \supseteq F$ is separable.

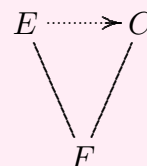
Proof. Consider first the case $\text{char } E = \text{char } F = 0$. Suppose $f(x) \in F[x]$ is monic irreducible, and write $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$ where $n \geq 1$ and $a_i \in F$. Suppose $\theta \in E$ is a root of $f(x)$; so $f(x)$ is the minimal polynomial of θ over F . Term-by-term differentiation shows that the derivative $f'(x) \in F[x]$ has leading term nx^{n-1} where the coefficient is nonzero (it is here that we require the hypothesis that $\text{char } F = 0$) and in particular $\deg f'(x) = n-1$. By minimality of the degree of the irreducible polynomial, $f'(\theta) \neq 0$. However if $f(x) = (x-\theta)^2g(x)$ where $g(x) \in E[x]$, then the derivative $f'(x) = (x-\theta)[(x-\theta)g'(x) + 2g(x)]$ has θ as a root. This is a contradiction.

A similar argument works if $E = \mathbb{F}_{q^r}$, $F = \mathbb{F}_q$, $q = p^e$, p prime, $r, e \geq 1$. Let $f(x) \in F[x]$ be monic irreducible of degree n ; and suppose $\theta \in E$ is a repeated root of $f(x)$. The argument above shows that $f'(\theta) = 0 \in F[x]$. In characteristic p this

simply means that every term in $f(x)$ has exponent divisible by p , so $n = rp$ and $f(x) = b_0 + b_1x^p + b_2x^{2p} + \cdots + b_rx^{rp} = g(x)^p$ where $g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_rx^r \in F[x]$ and $c_i = b_i^{p^{e-1}}$ using Theorem 3.7. But $\deg g(x) = r < n$ and evidently $g(\theta) = 0$, again contradicting the minimality of the degree of the minimal polynomial of θ over F . \square

Now let $E \supseteq F$ be an extension of degree n , and let C be an algebraically closed field containing F . (For example if $F = \mathbb{Q}$, one can take C to be \mathbb{C} or \mathbb{A} ; if F is a finite field of characteristic p , one can take $C = \bigcup_{k=1}^{\infty} \mathbb{F}_{p^k}$.) An **F -monomorphism** or **F -embedding** $\sigma : E \rightarrow C$ is an injective ring (or field) homomorphism satisfying $\sigma(a) = a$ for all $a \in F$.

Theorem A4.6. Let $E \supseteq F$ be a separable extension of degree n , and let C be an algebraically closed field containing F . Then there exist exactly n distinct F -monomorphisms from E into C .



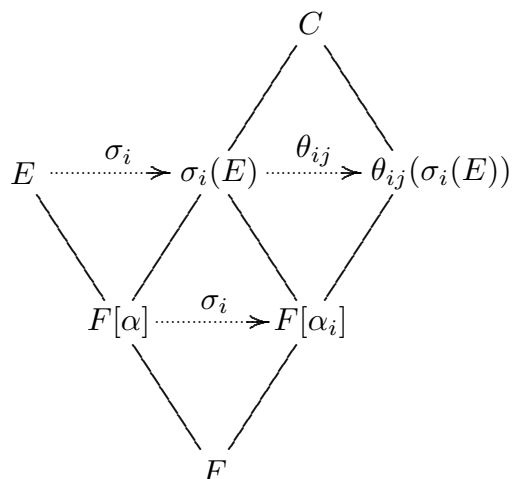
Proof. First consider the special case that $E = F[\alpha]$ for some $\alpha \in E$. Let $f(x) = \text{Irr}_{\alpha, F}(x)$. Since C is algebraically closed, $f(x)$ splits into linear factors in $C[x]$, say $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ where each $\alpha_i \in C$. For each i , observe that $\text{Irr}_{\alpha_i, F}(x) = f(x)$ since $f(x)$ is monic irreducible in $F[x]$ and has α_i as a root.

For each $i = 1, 2, \dots, n$, define $\sigma_i : F[\alpha] \rightarrow C$ by $g(\alpha) \mapsto g(\alpha_i)$ where $g(x) \in F[x]$. Then σ_i is well-defined, since if $g(\alpha) = h(\alpha)$, then $g(x) \equiv h(x) \pmod{f(x)}$, in which case $g(\alpha_i) = h(\alpha_i)$. Clearly $\sigma_i : E \rightarrow C$ is a ring homomorphism, fixing every element of F . Also σ_i is one-to-one, for if $\sigma_i(g(\alpha)) = g(\alpha_i) = 0$, then $f(x)$ divides $g(x)$, so that $g(\alpha) = 0$. So each $\sigma_i : E \rightarrow C$ is an F -monomorphism. The image of σ_i is the subfield $\sigma_i(E) = F[\alpha_i] \subseteq C$.

Now $F[\alpha_i] \cong F[\alpha] = E$ is separable over F , so $\alpha_1, \alpha_2, \dots, \alpha_n$ are distinct. Since $\sigma_i(\alpha) = \alpha_i$, the monomorphisms $\sigma_1, \sigma_2, \dots, \sigma_n$ are distinct.

Finally, let σ be any F -monomorphism from E into C . Then $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$, so that $\sigma(\alpha) \in \{\alpha_1, \alpha_2, \dots, \alpha_n\}$. Let us say that $\sigma(\alpha) = \alpha_i$. Since the ring homomorphisms σ and σ_i agree on F and on α , they must agree on $F[\alpha] = E$, i.e. $\sigma = \sigma_i$. Thus $\sigma_1, \sigma_2, \dots, \sigma_n$ are the *only* F -monomorphisms from E into C .

Consider now the general case $E \supset F$, and let $\alpha \in E \setminus F$. We may assume that $F[\alpha] \subset E$; otherwise we are done by the previous case. We have $E \supset F[\alpha] \supset F$ and $n = mt$ where $m = [E : F[\alpha]]$ and $t = [F[\alpha] : F]$. By induction on the degree of extension, there exist t distinct F -monomorphisms $\sigma_1, \sigma_2, \dots, \sigma_t : F[\alpha] \rightarrow C$. Let $\alpha_i = \sigma_i(\alpha)$.



Since $\sigma_i : E \rightarrow \sigma_i(E)$ is an F -isomorphism, the extension $\sigma_i(E) \supseteq F$ is separable; hence by Theorem A4.4, the extension $\sigma_i(E) \supseteq F[\alpha_i]$ is separable. By induction on the degree of extension, for each i there exist m distinct $F[\alpha_i]$ -monomorphisms $\theta_{i1}, \theta_{i2}, \dots, \theta_{im} : \sigma_i(E) \rightarrow C$. The composite maps $\theta_{ij} \circ \sigma_i : E \rightarrow C$ constitute $mt = n$ distinct F -monomorphisms. To see that these are the *only* F -monomorphisms $E \rightarrow C$, suppose that $\sigma : E \rightarrow C$ is an F -monomorphism. As before, σ must take α to some α_i . Then $\sigma \circ \sigma_i^{-1} : \sigma_i(E) \rightarrow C$ is an $F[\alpha_i]$ -monomorphism, so by induction, $\sigma \circ \sigma_i^{-1} = \theta_{ij}$ for some j , whence $\sigma = \theta_{ij} \circ \sigma_i$ as required. \square

As preparation for the next theorem, we require

Lemma A4.7. Let V be a vector space over an infinite field F . Then V is not a union of finitely many proper subspaces.

Proof. Suppose there exists a positive integer n for which there exists a vector space V covered by finitely many proper subspaces. We may further suppose n is minimal with this property; and now we seek a contradiction. Clearly $n > 1$; and there exists a vector space $V = V_1 \cup V_2 \cup \dots \cup V_n$ over F where each $V_i < V$ is a proper subspace. For each $i \in \{1, 2, \dots, n\}$, there exists $v_i \in V \setminus \bigcup_{j \neq i} V_j$ by minimality of n . It is easy to see that the affine line $L = \{v_1 + tv_2 : t \in F\}$ intersects each V_i in at most one point. However, L has an infinite number of points in $V = V_1 \cup V_2 \cup \dots \cup V_n$, a contradiction. \square

It is often useful to have a single generator for an extension field. The following result guarantees that such a generator exists for all finite separable extensions. We present a proof, however, only in the easiest cases which we care about most: finite fields and fields of characteristic zero. For a proof in the general case, see e.g. Garling [Ga]. This is usually called the **Theorem of the Primitive Element**, terminology that conflicts with usage

in the finite case, where a *primitive* element is a generator of the multiplicative group; so we would prefer to call this the **Theorem of Simple Extensions**.

Theorem A4.8. Let $E \supseteq F$ be a finite separable extension of fields. Then $E = F[\alpha]$ for some $\alpha \in E$.

Proof in the case $\text{char } F = 0$ *or* $|F| < \infty$. The finite field case is easy: just take α to be a generator of E^\times , by Theorem 3.2. Hence we assume the characteristic is zero. Let C be an algebraically closed field containing F . By Theorem A4.6, there exist distinct F -monomorphisms $\sigma_1, \sigma_2, \dots, \sigma_n : E \rightarrow C$ where $n = [E : F]$.

We claim that there exists $\alpha \in E$ such that the images $\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha) \in C$ are distinct. To see this, we apply Lemma A4.7 as follows. Whenever $1 \leq i < j \leq n$, the set $V_{ij} = \{x \in E : \sigma_i(x) = \sigma_j(x)\}$ is a proper subspace of the vector space E over F . Also $|F| = \infty$ since $\text{char } F = 0$. Since E cannot be covered by finitely many proper subspaces V_{ij} , there exists $\alpha \in E \setminus (\bigcup_{1 \leq i < j \leq n} V_{ij})$, and this α has the required property: $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ whenever $i \neq j$.

Since $[E : F] < \infty$, we have $F(\alpha) = F[\alpha]$ by Theorem A1.2. So we have a tower of extensions $E \supseteq F[\alpha] \supseteq F$ and $n = [E : F[\alpha]][F[\alpha] : F]$. Since the restrictions $\sigma_1, \dots, \sigma_n : F[\alpha] \rightarrow C$ are distinct F -monomorphisms, we have $n \leq [F[\alpha] : F]$ by Theorem A4.6. Therefore $[F[\alpha] : F] = n$ and $E = F[\alpha]$. \square

Remark: The use of an algebraically closed extension C in the proof of Theorem A4.8 was merely a convenient crutch, and was not really necessary. All that is really required is a finite normal extension of E , thereby avoiding reference to the Axiom of Choice.

Appendix A5: Field Automorphisms and Galois Theory

We give a very quick introduction to Galois theory, with a few key small examples. For more details and proofs, see e.g. [Ga], [Sa]. The following is a restatement of Theorems A4.5 and A4.8.

Theorem A5.1. Let $E \supseteq F$ be a finite extension. Assume either that E and F are finite fields, or that they have characteristic zero. Then

- (a) $E = F[\alpha]$ for some $\alpha \in E$, i.e. the extension is **simple**.
- (b) The extension $E \supseteq F$ is separable. Recall: this means that for every polynomial $f(x) \in F[x]$ which is irreducible in $F[x]$, the polynomial $f(x)$ has no repeated roots in E . □

Throughout this section, all finite extensions considered are assumed to satisfy the hypotheses (and therefore the conclusions) of Theorem A5.1.

Denote by $\text{Aut } E$ the group of all automorphisms of a field E . Two elements α and β in a field F are **algebraic conjugates** if there exists an automorphism $\sigma \in \text{Aut } E$ of some extension $E \supseteq F$ such that $\sigma(\alpha) = \beta$.

Theorem A5.2. Let $\sigma_1, \dots, \sigma_k \in \text{Aut } E$ be distinct automorphisms of a field E . Then $\sigma_1, \dots, \sigma_k$ are linearly independent functions $E \rightarrow E$.

Proof. The result is clear for $k = 1$ since each $\sigma \in \text{Aut } E$ is nonzero. Suppose that there exist distinct automorphisms $\sigma_1, \dots, \sigma_k \in \text{Aut } E$ which are linearly dependent over E ; we seek a contradiction. We may suppose our counterexample is minimal; so $k \geq 2$ and every set of $k - 1$ distinct automorphisms of E is linearly independent. By assumption, there exist $c_1, c_2, \dots, c_k \in E$, not all zero, such that

$$c_1\sigma_1 + c_2\sigma_2 + \cdots + c_k\sigma_k = 0.$$

In fact every $c_i \neq 0$ by minimality of k . Since $\sigma_1 \neq \sigma_2$, there exists $a \in E$ such that $\sigma_1(a) \neq \sigma_2(a)$. For every $x \in E$ we have

$$\begin{aligned} c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_k\sigma_k(x) &= 0; \\ c_1\sigma_1(ax) + c_2\sigma_2(ax) + \cdots + c_k\sigma_k(ax) &= 0. \end{aligned}$$

Multiply the first equation by $\sigma_1(a)$ and subtract the second equation to get

$$c_2(\sigma_2(a) - \sigma_1(a))\sigma_2(x) + c_3(\sigma_3(a) - \sigma_1(a))\sigma_3(x) + \cdots + c_k(\sigma_k(a) - \sigma_1(a))\sigma_k(x) = 0$$

for all $x \in E$. However, the coefficient of $\sigma_2(x)$ in this linear combination is nonzero, contrary to our assumption of the minimality of k . This is a contradiction as desired. \square

Let $E \supseteq F$ be a finite extension. An **F -automorphism** of E is an automorphism $\sigma \in \text{Aut } E$ such that $\sigma(a) = a$ for all $a \in F$. (This builds upon the terminology of Appendix A4: an F -automorphism is an F -monomorphism which is also surjective.) The group of all F -automorphisms of E is denoted $G(E/F)$. Clearly $G(E/F) \leq \text{Aut } E$ is a subgroup in general; and equality holds if F is the prime subfield of E (the unique smallest subfield of E).

Theorem A5.3. Let $E \supseteq F$ be a finite extension of fields, satisfying the assumptions of Theorem A5.1. Let $f(x) \in F[x]$, and let $\alpha_1, \dots, \alpha_k$ be the distinct roots of $f(x)$ in E . Then every $\sigma \in G(E/F)$ permutes $\alpha_1, \dots, \alpha_k$.

Proof. Denote $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ where $a_0, a_1, \dots, a_n \in F$. For each $i \in \{1, 2, \dots, k\}$, the image $\sigma(\alpha_i) \in E$ satisfies

$$\begin{aligned} f(\sigma(\alpha_i)) &= a_0 + a_1\sigma(\alpha_i) + a_2\sigma(\alpha_i)^2 + \dots + a_n\sigma(\alpha_i)^n \\ &= \sigma(a_0 + a_1\alpha_i + a_2\alpha_i^2 + \dots + a_n\alpha_i^n) = \sigma(0) = 0 \end{aligned}$$

by our hypotheses, so that $\alpha_i \in \{\alpha_1, \dots, \alpha_k\}$. Since σ is injective, it must therefore permute $\alpha_1, \dots, \alpha_k$. \square

Theorem A5.4. Let $E = F[\alpha] \supseteq F$ be an extension of degree n , and let $f(x)$ be the minimal polynomial of α over F . Let $\alpha_1, \alpha_2, \dots, \alpha_k$ be all the roots of $f(x)$ in E (these are distinct by Theorem A5.1). Then

- (i) $G(E/F)$ transitively permutes $\alpha_1, \alpha_2, \dots, \alpha_k$.
- (ii) The only $\sigma \in G(E/F)$ fixing any of the roots α_i is the identity. (In the language of permutation groups, $G(E/F)$ permutes the roots regularly, i.e. sharply transitively.)
- (iii) $|G(E/F)| = k \leq n$.

Proof. Let C be an algebraic closure of E . Then $f(x)$ has exactly n roots $\alpha_1, \alpha_2, \dots, \alpha_n \in C$; and these are distinct by Theorem A5.1. By assumption, exactly the first k of these roots lie in E . By Theorem A4.6., there are exactly n distinct F -monomorphisms $\sigma_i : E \rightarrow C$ where $\sigma_i(\alpha) = \alpha_i$, $i = 1, 2, \dots, n$. Of these, only $\sigma_1, \dots, \sigma_k$ have values in E ; so these are all the F -automorphisms of E . \square

Note that the heavy lifting in the last proof was accomplished by Theorem A4.6. This is also true of our next proof.

A finite extension $E \supseteq F$ for which equality holds with $|G(E/F)| = [E : F]$ is a **Galois extension**. In this case, $G = G(E/F)$ is the **Galois group** of the extension. Alternatively, one may characterize an extension as Galois iff it is finite, normal and separable. This equivalence is due to the following.

Theorem A5.5. Let $E \supseteq F$ be a finite extension satisfying the hypotheses of Theorem A5.1. Then $E \supseteq F$ is Galois iff it is normal, iff E is the splitting field of some polynomial $f(x) \in F[x]$. Assuming $E = F[\alpha_1, \alpha_2, \dots, \alpha_k]$ where $f(x) = \prod_{i=1}^k (x - \alpha_i) \in F[x]$ with distinct roots $\alpha_1, \alpha_2, \dots, \alpha_k \in E$, then $G(E/F)$ is faithfully represented as a group of permutations of these k roots. In particular, $|G(E/F)| \leq k!$.

Proof. First suppose E is the splitting field of $f(x) \in F[x]$ over F ; say $f(x) = \prod_{i=1}^k (x - \alpha_i) \in F[x]$ and $E = F[\alpha_1, \dots, \alpha_k]$. By Theorem A5.1, every $\sigma \in G(E/F)$ permutes the roots $\alpha_1, \dots, \alpha_k$; and since these roots generate E over F , distinct elements of $G(E/F)$ yield distinct permutations of the roots, and $|G(E/F)| \leq k!$. Let C be an algebraic closure of E , and let $n = [E : F]$. By Theorem A4.6, there are exactly n distinct F -monomorphisms $E \rightarrow C$; and all of these must map $E \rightarrow E$ since they permute the roots of $f(x)$, these being generators of E over F . So we obtain n distinct elements of $G(E/F)$, and the extension $E \supseteq F$ is Galois.

Conversely, suppose $E \supseteq F$ is normal. By Theorem A5.1, $E = F[\alpha]$ for some $\alpha \in F$. Let $f(x) \in F[x]$ be the minimal polynomial of α over F , so that $\deg f(x) = n = [E : F]$. Since E is normal and separable over F , $f(x) = \prod_{i=1}^n (x - \alpha_i)$ with distinct roots $\alpha_i \in E$. By Theorem A5.4, $G(E/F)$ permutes $\alpha_1, \alpha_2, \dots, \alpha_n$ transitively. \square

Quadratic field extensions are normal (and hence Galois). This is the field-theoretic analogue of the fact that in group theory, subgroups of index 2 are normal:

Example A5.6: Quadratic Extensions. Assuming the hypotheses of Theorem A5.1, every quadratic extension is Galois. Let $E \supset F$ be a quadratic extension, and let $\alpha \in E \setminus F$. Since $E \supseteq F[\alpha] \supset F$ where $[E : F] = 2$, we must have $E = F[\alpha]$. Let $f(x) \in F[x]$ be the minimal polynomial of α over F . Then $f(x)$ is quadratic with a root in E , so $f(x)$ has two distinct roots in E : $f(x) = (x - \alpha)(x - \alpha')$ where $\alpha, \alpha' \in E$. By Theorem A5.5, $E \supset F$ is Galois. This means that $G(E/F)$ is generated by an automorphism σ of order 2 interchanging $\alpha \leftrightarrow \alpha'$.

For $n \geq 3$, there exist both Galois and non-Galois extensions of degree n . The next two examples include both types for $n = 3$. A **cyclic extension** is a Galois extension with a cyclic Galois group; this is the case in Example A5.7.

Example A5.7: A Cyclic Cubic Extension. The polynomial $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ is irreducible over \mathbb{Q} (since it is irreducible over \mathbb{F}_2 and hence over \mathbb{Z}). Let $\alpha \in \mathbb{C}$ be a root of $f(x)$; so we have a cubic extension $E = \mathbb{Q}[\alpha] \supset \mathbb{Q}$. We compute

$$\begin{aligned}\alpha^3 &= 1 + 2\alpha - \alpha^2, \\ \alpha^4 &= \alpha + 2\alpha^2 - \alpha^3 = -1 - \alpha + 3\alpha^2, \\ \alpha^5 &= -\alpha - \alpha^2 + 3\alpha^3 = 3 + 5\alpha - 4\alpha^2, \\ \alpha^6 &= 3\alpha + 5\alpha^2 - 4\alpha^3 = -4 - 5\alpha + 9\alpha^2, \text{ etc.}\end{aligned}$$

By direct computation, we verify that $\beta := \alpha^2 - 2$ is also a root of f :

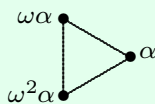
$$\begin{aligned}f(\beta) &= \beta^3 + \beta^2 - 2\beta - 1 \\ &= (\alpha^2 - 2)^3 + (\alpha^2 - 2)^2 - 2(\alpha^2 - 2) - 1 \\ &= (\alpha^6 - 6\alpha^4 + 12\alpha^2 - 8) + (\alpha^4 - 4\alpha^2 + 4) - 2(\alpha^2 - 2) - 1 \\ &= \alpha^6 - 5\alpha^4 + 6\alpha^2 - 1 = 0.\end{aligned}$$

Exactly the same reasoning shows that $\gamma := \beta^2 - 2 = (\alpha^2 - 2)^2 - 2 = 1 - \alpha - \alpha^2$ must be a root of $f(x)$. Since α, β, γ are algebraic of degree 3, they must be distinct; for example if $\beta = \alpha$ then α would satisfy a quadratic relation over \mathbb{Q} . We compute $\gamma^2 - 2 = \alpha$ and so $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha]$; therefore $E = \mathbb{Q}[\alpha] = \mathbb{Q}[\beta] = \mathbb{Q}[\gamma]$ is the splitting field of $f(x) = (x - \alpha)(x - \beta)(x - \gamma)$. The Galois group is $G = G(E/\mathbb{Q}) = \text{Aut } E = \langle \sigma \rangle$ where the automorphism σ cyclically permutes the roots as $\alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$.

By the Kronecker-Weber Theorem, every cyclic extension (being abelian) must be contained in a cyclotomic extension. The extension of Example A5.7 is the ‘simplest’ example of a cyclic extension of degree 3; it is a subfield of $\mathbb{Q}[\zeta_7]$ where we take $\alpha = \zeta_7 + \zeta_7^{-1}$; see Example 4.9.

Example A5.8: Galois Closure. The real number $\alpha = 2^{1/3}$ generates a cubic extension $K = \mathbb{Q}[\alpha] \supset \mathbb{Q}$. The minimal polynomial of α over \mathbb{Q} is $f(x) = x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$ where the quadratic factor is irreducible over K . The cubic extension $K \supset \mathbb{Q}$ is *not* Galois; $f(x)$ does not split into linear factors in $K[x]$, and the group $G(K/\mathbb{Q}) = \text{Aut } K$ is trivial, in accordance with Theorem A5.4.

The splitting field E of $f(x)$ is the **Galois closure** or **normal closure** of K , i.e. the smallest Galois extension of \mathbb{Q} containing K . Since $f(x) = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$ where $\omega = \zeta_3$, we have $E = \mathbb{Q}[\alpha, \omega]$. Note that $[E : \mathbb{Q}] = [E : K][K : \mathbb{Q}] = 2 \cdot 3 = 6$. The Galois group of the extension is $G = G(E/\mathbb{Q}) = \text{Aut } E = \langle \sigma, \tau \rangle$, a dihedral group of order 6 permuting the six roots in all $3! = 6$ possible ways. Here τ denotes complex conjugation $\omega \leftrightarrow \omega^2$ and fixing α ; σ cycles the three roots as $\alpha \mapsto \omega\alpha \mapsto \omega^2\alpha \mapsto \alpha$ while fixing ω . The three roots of $f(x)$ form the vertices of an equilateral triangle embedded in \mathbb{C} , on which G induces the full group of symmetries:



τ reflects across the horizontal axis of symmetry;
 σ rotates 120° counter-clockwise about the center

Of course σ *does not* rotate the entire complex plane—it fixes all points of \mathbb{Q} . The only elements of G acting continuously on E are ι and τ .

Example A5.9: An Abelian Quartic Extension. Let $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$. We show that this is a simple extension generated by $\alpha = \sqrt{2} + \sqrt{3}$, an algebraic integer of degree 4. Direct computation shows that α is a root of $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Clearly $f(x)$ has no linear factors in $\mathbb{Z}[x]$, since it has no roots in \mathbb{Z} (indeed, no roots in \mathbb{F}_3). It has six monic quadratic factors in $\mathbb{C}[x]$:

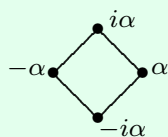
$$f(x) = (x^2 + 2\sqrt{2}x - 1)(x^2 - 2\sqrt{2}x - 1) = (x^2 + 2\sqrt{3}x + 1)(x^2 - 2\sqrt{3}x + 1) = (x^2 - 5 + 2\sqrt{6})(x^2 - 5 - 2\sqrt{6})$$

but none of these factors are in $\mathbb{Q}[x]$ since $\sqrt{2}, \sqrt{3}, \sqrt{6}$ are all irrational. It follows that $f(x)$ is irreducible in $\mathbb{Q}[x]$. From these factorizations it also follows that $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \subseteq \mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ so $E = \mathbb{Q}[\alpha]$ is a quartic extension of \mathbb{Q} as claimed. The four roots of $f(x)$ are $\pm\sqrt{2} \pm \sqrt{3} \in E$, so E is the splitting field of $f(x)$, hence a Galois extension of \mathbb{Q} .

Let $G = G(E/\mathbb{Q}) = \text{Aut } E$, so that $|G| = [E : \mathbb{Q}] = 4$. Every automorphism of E is determined by its action on the generators $\sqrt{2}$ and $\sqrt{3}$; but there are only four possible combinations of sign changes $\sqrt{2} \mapsto \pm\sqrt{2}, \sqrt{3} \mapsto \pm\sqrt{3}$; so all four of these combinations must yield automorphisms of E . So we must have a Klein four-group $G = \langle \sigma, \tau \rangle = \{ \iota, \sigma, \tau, \sigma\tau \}$ where $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sqrt{3}; \tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}$. Here $\iota = \text{id}$ and $\sigma\tau(\sqrt{2}) = -\sqrt{2}, \sigma\tau(\sqrt{3}) = -\sqrt{3}$, so $\sigma\tau(\sqrt{6}) = \sqrt{6}$.

Our convention here is to compose automorphisms right-to-left, thus $\sigma\tau = \sigma \circ \tau$. (In other expositions where composition is left-to-right, this will generally be evident from the superscript notation used for automorphisms, as in $a^{\sigma\tau} = (a^\sigma)^\tau$.)

Example A5.10: A Galois Extension Admitting the Dihedral Group of Order 8. The polynomial $f(x) = x^4 - 2 \in \mathbb{Z}[x]$ is irreducible over \mathbb{Q} by Eisenstein's Criterion A2.4. Its roots are $\pm\alpha, \pm i\alpha$ where $i = \sqrt{-1}$ and $\alpha = 2^{1/4}$. The splitting field of $f(x)$ over \mathbb{Q} is therefore $E = \mathbb{Q}[\alpha, i] = \mathbb{Q}[\alpha, \zeta]$ where $\zeta = \zeta_8 = \frac{1+i}{\sqrt{2}}$. Note that $E = K[i]$ where $K = \mathbb{Q}[\alpha]$ so $[E : \mathbb{Q}] = [E : K][K : \mathbb{Q}] = 2 \cdot 4 = 8$. The Galois group $G = G(E/\mathbb{Q}) = \text{Aut } E = \langle \sigma, \tau \rangle$ is dihedral of order 8 where τ is complex conjugation; $\sigma(i) = i$ and σ permutes the four roots of $f(x)$ cyclically as $\alpha \mapsto i\alpha \mapsto -\alpha \mapsto -i\alpha \mapsto \alpha$. Thus G permutes the four vertices of a square embedded in the complex plane as shown:



τ reflects across the horizontal axis of symmetry;
 σ rotates the four roots 90° counter-clockwise about the center

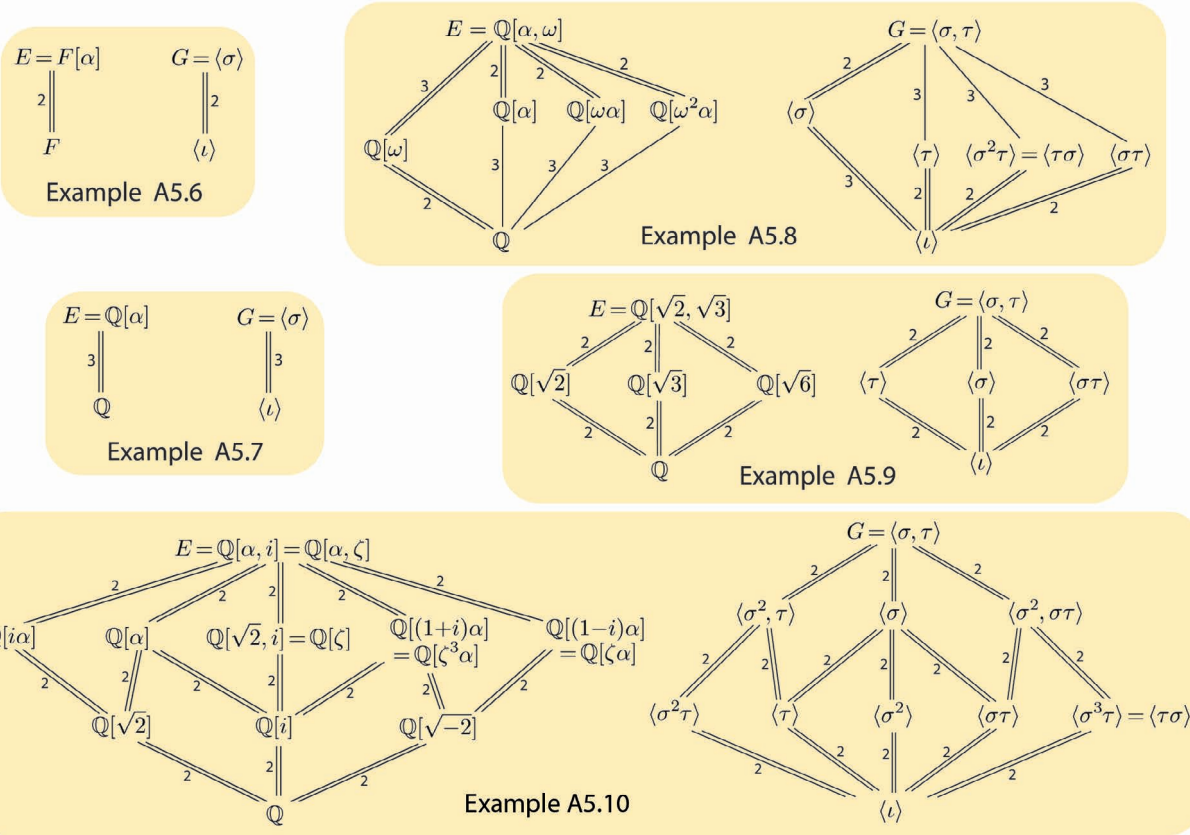
Let $E \supseteq F$ be a Galois extension with Galois group $G = G(E/F)$. Galois theory gives a beautiful description of all the intermediate fields K (i.e. $E \supseteq K \supseteq F$), establishing a one-to-one correspondence with the subgroups of G . A priori, it may not even be clear why the number of intermediate fields K should even be finite, or whether there should be any effective means of listing them all; but since G is a finite group, G has only finitely many subgroups and these can be effectively enumerated, thereby giving the exact number of subfields and their explicit description. This bijection, known as the **Galois correspondence**, is naturally defined as follows:

$$\begin{aligned} \left\{ \begin{array}{l} \text{intermediate fields } K : \\ E \supseteq K \supseteq F \end{array} \right\} &\longleftrightarrow \{ \text{subgroups } H \leq G \} \\ K &\longmapsto G_K = \left\{ \begin{array}{l} \sigma \in G : \sigma(a) = a \\ \text{for all } a \in K \end{array} \right\} \\ \text{Fix}_E(H) = \left\{ \begin{array}{l} a \in E : \sigma(a) = a \\ \text{for all } a \in H \end{array} \right\} &\longleftarrow H \\ &= \text{fixed subfield of } H \text{ (in } E) \end{aligned}$$

Theorem A5.11 (Fundamental Theorem of Galois Theory). Let $E \supseteq F$ be a Galois extension, with Galois group G . Then the correspondence defined above is a bijection between the intermediate subfields K satisfying $E \supseteq K \supseteq F$, and the subgroups $H \leq G$. It satisfies

- (i) The correspondence is order-reversing. Thus given intermediate subfields K, K' , we have $K \supseteq K'$ iff $G_K \leq G_{K'}$. Equivalently, given subgroups $H, H' \leq G$, we have $H \leq H'$ iff $\text{Fix}_E(H) \supseteq \text{Fix}_E(H')$.
- (ii) Assuming containments as in (i), the subgroup index equals the degree of extension: $[K : K'] = [G_{K'} : G_K]$.
- (iii) $G_E = \{\iota\}$; $G_F = G$; $\text{Fix}_E(G) = F$; $\text{Fix}_E(\{\iota\}) = E$ where $\iota = \text{id} \in G$.
- (iv) Assuming containments as in (i), normality for subgroup containment is equivalent to normality for the corresponding field extension. That is, the extension $K \supseteq K'$ is normal iff $G_K \trianglelefteq G_{K'}$. In this case, $K \supseteq K'$ is Galois with group $G(K/K') \cong G_{K'}/G_K$.

We illustrate the Galois correspondence in Examples A5.6–10 by presenting the **Hasse diagram** of intermediate fields in each case, side by side with the Hasse diagram of subgroups of the Galois group. Containment is depicted using vertical lines in each case. Double lines indicate normality; and the vertical lines are labelled by the corresponding index or degree. In each case, the Hasse diagram of subfields is obtained from the Hasse diagram of subgroups by inverting top-to-bottom (but preserving left and right).



The following application of Galois theory is typical: we want to justify why certain (given) elements of E lie in a desired subfield. Given a Galois extension $E \supseteq F$, Theorem A5.11 says that an element $a \in E$ is fixed by every element of $G = G(E/F)$ iff $a \in F$. See Appendix A7 for symmetric multivariate polynomials.

Theorem A5.12. Let $E \supseteq F$ be a Galois extension, and $G = G(E/F)$ its Galois group. For all $\alpha \in E$, we have $\sum_{\sigma \in G} \sigma(\alpha) \in F$ and $\prod_{\sigma \in G} \sigma(\alpha) \in F$. More generally, all symmetric polynomials in the algebraic conjugates of α lie in F .

Proof. Let $s(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$ be a symmetric polynomial in $n = |G|$ indeterminates with coefficients in F . Denoting $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$, the element $s(\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)) \in E$ is fixed by every $\sigma_i \in G$, since σ_i permutes the n arguments of s . (These arguments are the algebraic conjugates of α , each listed the same number of times—they are not assumed to be distinct.) By Theorem A5.11(iii), $s(\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)) \in \text{Fix}_E(G) = F$. \square

Theorem A5.13. Let $K \supseteq F$ be a Galois extension with group $G = G(K/F)$. Then the norm and trace maps of the extension satisfy

$$N_{K/F} \alpha = \prod_{\sigma \in G} \sigma(\alpha), \quad \text{Tr}_{K/F} \alpha = \sum_{\sigma \in G} \sigma(\alpha) \quad \text{for all } \alpha \in K.$$

Proof. Let $f(x) \in F[x]$ be the minimal polynomial of α over F , and let $n = \deg f(x)$. Let $E = F[\alpha]$, so that $[E : F] = n$ and $[K : F] = mn$ where $m = [K : E]$. Since the extension $K \supseteq F$ is Galois, $f(x)$ splits into linear factors in $K[x]$ and there exist $\tau_1, \tau_2, \dots, \tau_n \in G$ such that $\tau_1(\alpha), \tau_2(\alpha), \dots, \tau_n(\alpha) \in K$ are the roots of $f(x)$. (Note that the roots do not necessarily lie in E .) Now

$$f(x) = \prod_{i=1}^n (x - \tau_i(\alpha)) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \dots + (-1)^n a_n \in F[x].$$

By Theorem A5.11, $|G_K| = m$ and $[G : G_K] = n$ where G_K is the set of all $\sigma \in G$ fixing every element in K . The n left cosets of G_K in G must be $\tau_1 G_K, \tau_2 G_K, \dots, \tau_n G_K$ since $\tau_i G_K \cap \tau_j G_K = \emptyset$ whenever $i \neq j$ (since the images $\tau_i(\sigma(\alpha)) = \tau_i(\alpha)$ are distinct for $i = 1, 2, \dots, n$ where $\sigma \in G_K$). Thus

$$\prod_{\sigma \in G} \sigma(\alpha) = \prod_{i=1}^n \prod_{\sigma \in G_K} \tau_i(\sigma(\alpha)) = \prod_{i=1}^n \tau_i(\alpha)^m = a_n^m = (N_{E/F} \alpha)^m = N_{K/F} \alpha$$

and

$$\sum_{\sigma \in G} \sigma(\alpha) = \sum_{i=1}^n \sum_{\sigma \in G_K} \tau_i(\sigma(\alpha)) = m \sum_{i=1}^n \tau_i(\alpha) = m a_1 = m \text{Tr}_{E/F} \alpha = \text{Tr}_{K/F} \alpha$$

by Corollary A1.10. □

Corollary A5.14. Let $E \supseteq F$ be a Galois extension, and let $\alpha \in E$. Then all algebraic conjugates of α have the same trace; and they all have the same norm.

Proof. Let $G = G(E/F)$. Every algebraic conjugate of α has the form $\tau(\alpha) \in E$ for some $\tau \in G$. Then

$$\mathrm{Tr}_{E/F}(\tau(\alpha)) = \sum_{\sigma \in G} \sigma(\tau(\alpha)) = \sum_{\rho \in G} \rho(\alpha) = \mathrm{Tr}_{E/F}(\alpha)$$

by Theorem A5.13, after substituting $\rho = \sigma\tau$. The argument for norms is similar. □

Now consider a Galois extension $E \supseteq F$ of degree n with group $G = G(E/F)$. A **normal basis** for E over F is a basis $\mathcal{B} = \{\beta_1, \beta_2, \dots, \beta_n\}$ for E over F which is permuted transitively by G , i.e. $\mathcal{B} = \{\sigma(\beta) : \sigma \in G\}$ where $\beta = \beta_1$. The size $|G| = n$ is just right to make this seem possible. For instance, if we choose $\beta \in \mathbb{Q}[i]$ to be neither real nor pure imaginary, then $\{\beta, \bar{\beta}\}$ is a normal basis for the extension $\mathbb{Q}[i] \supset \mathbb{Q}$. This example shows that it is not sufficient to take β to satisfy $E = F[\beta]$; but, a ‘random’ (or generic) choice of $\beta \in E$ seems like it should work. Nevertheless, it is tricky to prove the existence of a normal basis in general!

Theorem A5.15 (Normal Basis Theorem). Let $E \supseteq F$ be a Galois extension satisfying the hypotheses of Theorem A5.1. Then there exists a normal basis for E over F .

Proof. First consider the case that $E = \mathbb{F}_{q^n}$, $F = \mathbb{F}_q$. By Theorem 3.8, $G = G(E/F) = \{\iota, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ where $\sigma(x) = x^q$ and $\sigma^n = \iota$. Regarding σ as an F -linear transformation $E \rightarrow E$ at the moment, its minimal polynomial $m(x) \in F[x]$ must divide $x^n - 1$. But if $\deg m(x) < n$, this would give a nontrivial F -linear combination of $\iota, \sigma, \sigma^2, \dots, \sigma^{n-1}$ equal to zero, contrary to Theorem A5.2. This cannot happen; so $\deg m(x) = n$. This means that $m(x)$ coincides with the characteristic polynomial of σ on E . Thus E is a cyclic $F[\sigma]$ -module, i.e. there exists $\beta \in E$ such that $\{\beta, \sigma(\beta), \sigma^2(\beta), \dots, \sigma^{n-1}(\beta)\}$ spans E over F , thereby forming a normal basis as required. See e.g. [HH, Chapter 11] for relevant results from linear algebra.

It remains to consider the case E and F have characteristic zero; in particular they are infinite fields. Here we paraphrase Artin’s proof [Ar]. By Theorem A5.1, $E = F[\alpha]$ for some $\alpha \in E$. Let $f(x) \in F[x]$ be the minimal polynomial of α over F , so that

$\deg f(x) = n = [E : F] = |G|$ and $f(x) = \prod_{\sigma \in G} (x - \sigma(\alpha))$. For each $\tau \in G$ consider the polynomial

$$g_\tau(x) = \prod_{\substack{\sigma \in G \\ \sigma \neq \tau}} \frac{x - \sigma(\alpha)}{\tau(\alpha) - \sigma(\alpha)} \in E[x]$$

of degree $n - 1$ (noting that the n roots of $f(x)$ are distinct so there is no division by zero here). The reader may recognize these n polynomials as the Lagrange interpolation basis for the polynomials of degree $n - 1$ at the roots of $f(x)$: the polynomial $g_\tau(x)$ vanishes at all the roots of $f(x)$ except at $\tau(\alpha)$, where it has value 1 (see Theorem 3.12). Now it follows that

$$(A5.16) \quad \sum_{\tau \in G} g_\tau(x) = 1$$

since the polynomial on the left has degree at most $n - 1$, but by the preceding comments it evaluates to 1 at each of the n distinct roots of $f(x)$. Also in $E[x]$ we have

$$(A5.17) \quad g_\tau(x)g_\rho(x) \equiv \begin{cases} 0 \pmod{f(x)}, & \text{if } \tau \neq \rho \text{ in } G; \\ g_\tau(x) \pmod{f(x)}, & \text{if } \tau = \rho \text{ in } G. \end{cases}$$

The first congruence follows since $g_\tau(x)g_\rho(x)$ vanishes at all of the n roots of $f(x)$ whenever $\tau \neq \rho$. When $\tau = \rho$, multiplying both sides of (A5.16) by $g_\tau(x)$ yields $g_\tau(x)^2 \equiv g_\tau(x) \pmod{f(x)}$. Considering now the action of G on $E[x]$ via its natural action on coefficients, one easily finds that

$$(A5.18) \quad G \text{ permutes the } n \text{ polynomials } g_\tau(x) \text{ for } \tau \in G, \text{ in the same way that } G \text{ permutes the } n \text{ roots of } f(x) \text{ (i.e. they are equivalent } G\text{-sets). In fact, } \sigma(g_\tau(x)) = g_{\sigma\tau}(x) \text{ for all } \sigma, \tau \in G.$$

Now consider the $n \times n$ matrix $M(x)$ with rows and columns indexed by elements of G , having (σ, τ) -entry equal to the polynomial $g_{\sigma\tau}(x) \in E[x]$. Since $M(x)$ is an $n \times n$ matrix with entries in $E[x]$, its determinant is also a polynomial in x (in fact, of degree at most $n(n - 1)$). We will show that $\det M(x) \neq 0$, by showing that $\det(M(x)^T M(x)) = (\det M(x))^2 \equiv 1 \pmod{f(x)}$. The (σ, τ) -entry of $M(x)^T M(x)$ is

$$\sum_{\rho \in G} g_{\rho\sigma}(x)g_{\rho\tau}(x) = \sum_{\rho \in G} \rho(g_\sigma(x)g_\tau(x)) \equiv 0 \pmod{f(x)}$$

if $\sigma \neq \tau$, by (A5.17); whereas for $\sigma = \tau$,

$$\sum_{\rho \in G} g_{\rho\sigma}(x)g_{\rho\sigma}(x) = \sum_{\rho \in G} g_\rho(x)^2 \equiv \sum_{\rho \in G} g_\rho(x) \equiv 1 \pmod{f(x)}.$$

Thus in $E[x]$ we have $\det M(x)^2 \equiv 1 \pmod{f(x)}$ and, in particular, $\det M(x)$ is a *nonzero* polynomial. Since F is an infinite field, there exists $a \in F$ such that $\det M(a) \neq 0$. Take

$\mathcal{B} = \{g_\tau(a) : \tau \in G\}$. For all $\sigma \in G$ we have $\sigma(a) = a$ and so $\sigma(g_\tau(a)) = g_{\sigma\tau}(a)$; thus G acts on \mathcal{B} . It remains to be shown that \mathcal{B} is a basis for E over F . Suppose that $\sum_{\tau \in G} c_\tau g_\tau(a) = 0$ for some constants $c_\tau \in F$. Applying an arbitrary $\sigma \in G$ to this equation yields

$$0 = \sum_{\tau \in G} \sigma(c_\tau g_\tau(a)) = \sum_{\tau \in G} g_{\sigma\tau}(a) c_\tau$$

so the vector $(c_\tau : \tau \in G)$ is in the null space of the nonsingular matrix $M(a)$. This forces $c_\tau = 0$ for all τ , so \mathcal{B} is a basis. \square

Appendix A6: Dedekind Zeta Functions and Dirichlet Series

Let E be a number field with ring of integers $\mathcal{O} = \mathcal{O}_E$. The **Dedekind zeta function** of E is the complex-valued function

$$\zeta_E(s) = \sum_{0 \neq \mathcal{A} \subseteq \mathcal{O}} \frac{1}{N(\mathcal{A})^s}$$

where the sum extends over all nonzero ideals $\mathcal{A} \subseteq \mathcal{O}$, and $N(\mathcal{A}) = |\mathcal{O}/\mathcal{A}|$ is the norm of \mathcal{A} . The series converges for complex numbers s with $\Re(s) > 1$; but by analytic continuation, the function has a meromorphic extension to \mathbb{C} with a simple pole at $s = 1$. It has an **Euler factorization** given by

$$\zeta_E(s) = \prod_{\mathfrak{P}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1},$$

also convergent for $\Re(s) > 1$; the product extends over all nonzero prime ideals $\mathfrak{P} \subset \mathcal{O}$. The theorem equating the infinite series with the infinite product, can readily be seen as an algebraic reformulation of the fact that every nonzero ideal $\mathcal{A} \subseteq \mathcal{O}$ factors uniquely as a product of prime ideals (although the details relating convergence requires a little more care than we provide here).

Example A6.1: The Riemann Zeta Function. For $E = \mathbb{Q}$, the Dedekind zeta function coincides with the Riemann Zeta Function: $\zeta_{\mathbb{Q}}(s) = \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Its Euler factorization is $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ where the product extends over all rational primes p .

The zeta functions of Dedekind are the most typical zeta functions of number theory; and although not required in our Section 12, this appendix is intended to provide motivational context for our discussion there. Here the student may see something of the larger role of zeta functions for studying the distribution of primes in Dedekind domains. Another reason for including this Appendix is to provide an additional application (Dirichlet's Theorem A6.2 below) of the character theory of finite abelian groups of Section 6.

A **Dedekind domain** is an integral domain in which every nonzero ideal factors uniquely as a product of prime ideals. The two main examples are the ring \mathcal{O}_E of integers in a number field E ; and the ring of polynomials $\mathcal{O}_E = F[x_1, x_2, \dots, x_n]$ in a function field $E = F(x_1, x_2, \dots, x_n)$. In both cases E is the field of fractions of \mathcal{O}_E . Questions regarding the distribution of primes in \mathcal{O}_E are best studied by rephrasing them in terms of the behavior of $\zeta_E(s)$ (particularly the zeroes and poles of this zeta function). Often these questions are too difficult to solve in the number field case (witness the Riemann hypothesis); and then one turns to the function field case where the questions are typically

more manageable, hoping for inspiration that might apply in the number field case. Thus for example, the very precise formula of Theorem 3.13 counting irreducible polynomials of each degree (and thereby prime ideals of a given norm) in $\mathbb{F}_q[x]$, has a clear analogue for the prime-counting function $\pi(x) = |\{\text{prime } p \in \mathbb{N} : p \leq x\}|$ which we can state as a conjecture, but are currently unable to prove except in a weaker asymptotic sense.

Theorem A6.2 (Dirichlet). Let a and N be relatively prime positive integers. Then there exist infinitely many (rational) primes $p \equiv a \pmod{N}$.

Let $G = (\mathbb{Z}/N\mathbb{Z})^\times$, the multiplicative group of units of the ring of integers mod N ; so $|G| = n := \phi(N)$. For each character $\chi \in \widehat{G}$, compose χ with the canonical projection $k \mapsto k + N\mathbb{Z}$ in order to lift χ to a map $\chi : \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$. We write $\chi(k) = 0$ whenever $\gcd(k, N) \neq 1$; and $\chi(k) \in \langle \zeta_n \rangle$ as before, if $\gcd(k, N) = 1$. This extension of $\chi \in \widehat{G}$ to a function $\mathbb{Z} \rightarrow \mathbb{C}$, while not exactly a linear character as defined in Section 6, is *completely multiplicative* (i.e. $\chi(k\ell) = \chi(k)\chi(\ell)$ for all $k, \ell \in \mathbb{Z}$). It is called a **Dirichlet character** modulo N . Each character $\chi \in \widehat{G}$ (lifted to \mathbb{Z}) yields a **Dirichlet L -function**

$$(A6.3) \quad L_\chi(s) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}, \text{ where } s \in \mathbb{C}.$$

As with the Riemann zeta function of Example A6.1, the series (A6.3) converges for $\Re s > 1$ but admits an analytic continuation to a meromorphic function on $\mathbb{C} \setminus \{1\}$. And for exactly the same reasons as in the zeta function case, we obtain an Euler factorization

$$L_\chi(s) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

convergent at least for $\Re s > 1$. (Here and throughout, the index p varies over all rational primes.) While the function $L_\chi(s)$ has complex values in general, we can safely restrict s to real values > 1 for the argument at hand. Here, all Euler factors have values in the right half-plane where we can take the standard branch of natural logarithm; thus

$$\ln L_\chi(x) = - \sum_p \ln \left(1 - \frac{\chi(p)}{p^x}\right), \quad \text{for } x > 1.$$

We require the Taylor expansion of each of these terms, found by integrating $\frac{1}{1-u} = 1 + u + u^2 + u^3 + \dots$ (for $|u| < 1$) to obtain

$$-\ln(1-u) = u + \frac{u^2}{2} + \frac{u^3}{3} + \frac{u^4}{4} + \dots = \sum_{k=1}^{\infty} \frac{u^k}{k}, \quad \text{for } |u| < 1.$$

Using this in the previous formula gives the series expansion

$$(A6.4) \quad \ln L_\chi(x) = \sum_p \sum_{k=1}^{\infty} \frac{\chi(p)^k}{kp^{kx}} = \sum_p \frac{\chi(p)}{p^x} + \sum_p \sum_{k=2}^{\infty} \frac{\chi(p)^k}{kp^{kx}}.$$

The dominant terms in (A6.4) are those in the first sum $\sum_p \frac{\chi(p)}{p^x}$. To see that the remaining terms are small (their total contribution is uniformly bounded for all $x > 1$), we note that

$$\begin{aligned} \left| \sum_p \sum_{k=2}^{\infty} \frac{\chi(p)^k}{kp^{kx}} \right| &\leq \sum_p \sum_{k=2}^{\infty} \frac{1}{kp^{kx}} \leq \frac{1}{2} \sum_p \frac{1}{(p^x)^2} \\ &\leq \frac{1}{2} \sum_{r=2}^{\infty} \frac{1}{r^2} = \frac{1}{2} \left(\frac{\pi^2}{6} - 1 \right) < 1 \quad \text{for all } x > 1. \end{aligned}$$

Using orthogonality of characters from Theorem 6.2(b), we have

$$(A6.5) \quad \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \chi(k) = \begin{cases} n, & \text{if } k \equiv a \pmod{N}; \\ 0, & \text{otherwise} \end{cases} \quad \text{for } x > 1.$$

When applied to (A6.4), this yields

$$(A6.6) \quad \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \ln L_\chi(x) = \sum_p \sum_{\chi \in \widehat{G}} \frac{\overline{\chi(a)} \chi(p)}{p^x} + O(1) = \sum_{p \equiv a \pmod{N}} \frac{1}{p^x} + O(1) \quad \text{as } x \rightarrow 1^+$$

using (A6.5) for all terms with $\gcd(k, N)=1$; and we recall that the terms with $\gcd(k, N)>1$ give $\chi(k) = 0$. Here ‘ $O(1)$ ’ stands for terms that are uniformly bounded (it has absolute value at most n , whatever the value of $x > 1$; this follows from (A6.4) and the estimate which follows it). We see that the Dirichlet characters succeed in filtering out individual congruence classes within the sequence of primes, thereby bringing us closer to our goal.

We now investigate the behaviour of each of the functions $L_\chi(x)$ as $x \rightarrow 1^+$. We first show that

$$(A6.7) \quad \text{for the trivial character } \chi \in \widehat{G}, \text{ we have } L_\chi(x) \rightarrow \infty \text{ as } x \rightarrow 1^+.$$

For in this case

$$L_\chi(x) = \sum_{\gcd(k, N)=1} \frac{1}{k^x} \geq \sum_{k \equiv 1 \pmod{N}} \frac{1}{k^x} = \sum_{r=1}^{\infty} \frac{1}{(rN+1)^x} \rightarrow \infty \quad \text{as } x \rightarrow 1^+$$

by comparison with

$$\int_1^{\infty} \frac{dt}{(tN+1)^x} = \frac{1}{(x-1)N(N+1)^{x-1}} \rightarrow \infty \quad \text{as } x \rightarrow 1^+.$$

Now consider an arbitrary nontrivial character $\chi \in \widehat{G}$, and we must show that $L_\chi(x)$ remains bounded as $x \rightarrow 1^+$. In this case we break up the positive integers into intervals of size N , thus:

$$\begin{aligned}
 \text{(A6.8)} \quad L_\chi(x) &= \sum_{k=1}^{\infty} \frac{\chi(k)}{k^x} = \sum_{r=0}^{\infty} \sum_{k=1}^N \frac{\chi(k)}{(rN+k)^x} \\
 &= \sum_{r=0}^{\infty} \left(\sum_{k=1}^N \frac{\chi(k)}{(rN+N)^x} + \sum_{k=1}^N \chi(k) \left[\frac{1}{(rN+k)^x} - \frac{1}{(rN+N)^x} \right] \right) \\
 &= \sum_{r=0}^{\infty} \sum_{k=1}^N \chi(k) \left[\frac{1}{(rN+k)^x} - \frac{1}{(rN+N)^x} \right]
 \end{aligned}$$

since $\sum_{k=1}^N \chi(k) = 0$ by orthogonality of characters from Theorem 6.2(a). Now bound the inner sum by

$$\begin{aligned}
 \text{(A6.9)} \quad \left| \sum_{k=1}^N \chi(k) \left[\frac{1}{(rN+k)^x} - \frac{1}{(rN+N)^x} \right] \right| &\leq \sum_{k=1}^N \left[\frac{1}{(rN+k)^x} - \frac{1}{(rN+N)^x} \right] \\
 &\leq N \left[\frac{1}{(rN+1)^x} - \frac{1}{(rN+N)^x} \right].
 \end{aligned}$$

Denoting $f(u) = u^{-x}$ for $u > 0$, the Mean Value Theorem yields

$$f(rN+1) - f(rN+N) = f'(\xi)(1-N) = (N-1)x\xi^{-x-1} \leq \frac{(N-1)x}{(rN+1)^{x+1}} \leq \frac{(N-1)x}{(rN+1)^2}$$

for some ξ between $rN+1$ and $rN+N$, where $x > 1$. Using this in (A6.9) and substituting into (A6.8) gives

$$|L_\chi(x)| \leq N(N-1)x \sum_{r=0}^{\infty} \frac{1}{(rN+1)^2} \leq N(N-1)x \sum_{\ell=1}^{\infty} \frac{1}{\ell^2} = \frac{N(N-1)x\pi^2}{6}.$$

This finally gives

$$\text{(A6.10)} \quad \text{for every nontrivial character } \chi \in \widehat{G}, |L_\chi(x)| \text{ remains bounded as } x \rightarrow 1^+.$$

We are now ready to prove Theorem A6.2, arguing by contradiction. Suppose there are only finitely many primes $p \equiv a \pmod{N}$. Then the right side of (A6.6) is bounded as $x \rightarrow 1^+$ (because the $O(1)$ terms are bounded; and the other sum converges to $\sum \left\{ \frac{1}{p} : \text{primes } p \equiv a \pmod{N} \right\}$, a finite sum by assumption). Therefore the left side of (A6.6) must also remain bounded as $x \rightarrow 1^+$. The terms $\overline{\chi(a)} \ln L_\chi(x)$ for nontrivial χ certainly remain bounded as $x \rightarrow 1^+$, by (A6.10). However for the trivial character χ , the term $|\overline{\chi(a)} \ln L_\chi(x)| \rightarrow \infty$ as $x \rightarrow 1^+$, by (A6.7). This is the desired contradiction; so Theorem A6.2 follows. \square

Appendix A7: Symmetric Polynomials

Let F be a field. A multivariate polynomial $s(x_1, x_2, \dots, x_n) \in F[x_1, x_2, \dots, x_n]$ is **symmetric** if it is unchanged under all $n!$ permutations of the coordinates. Examples include the **elementary symmetric polynomials**

$$e_k = e_k(x_1, x_2, \dots, x_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}, \quad k \in \{0, 1, 2, \dots, n\}.$$

Note that $e_k(x_1, \dots, x_n)$ has $\binom{n}{k}$ terms, these being the products of all k -subsets of the n indeterminates. In particular,

$$e_0(x_1, \dots, x_n) = 1, \quad e_1(x_1, \dots, x_n) = x_1 + x_2 + \cdots + x_n, \quad e_n(x_1, \dots, x_n) = x_1 x_2 \cdots x_n$$

and $e_k = 0$ for $k \notin \{0, 1, 2, \dots, n\}$. From the definition, one readily deduces the identity

$$\prod_{i=1}^n (t - x_i) = t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^n e_n$$

in $F[x_1, \dots, x_n, t]$, and so this product serves as a generating function for the elementary symmetric polynomials. It also shows that the coefficients in any univariate polynomial are (up to signs) the elementary symmetric polynomials in its roots.

Another important set of symmetric polynomials is the set of **moment polynomials** or **power sum polynomials**

$$m_k = m_k(x_1, x_2, \dots, x_n) = x_1^k + x_2^k + \cdots + x_n^k, \quad k \in \{0, 1, 2, \dots\}$$

(and in particular $m_0 = n$). A famous set of relations allows us to recursively express the moment polynomials in terms of the elementary symmetric polynomials (and often conversely, but see the later comments):

Theorem A7.1 (Newton's Identities). For all $k \geq 0$,

$$\begin{aligned} e_1 &= m_1 \\ 2e_2 &= m_1 e_1 - m_2 \\ 3e_3 &= m_1 e_2 - m_2 e_1 + m_3 \\ &\vdots \\ k e_k &= \sum_{i=1}^k (-1)^{i+1} m_i e_{k-i} \end{aligned}$$

Proof. In the field $F((x_1, x_2, \dots, x_n, t))$ we have

$$\begin{aligned} \left(\sum_{i=0}^{\infty} m_i t^i \right) \left(\sum_{j=0}^{\infty} (-1)^j e_j t^j \right) &= \left(\sum_{i=1}^n \frac{1}{1 - x_i t} \right) \prod_{j=1}^n (1 - x_j t) \\ &= \sum_{i=1}^n \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (1 - x_j t) = \sum_{j=0}^{n-1} (-1)^j (n-j) e_j t^j. \end{aligned}$$

The last equality holds because in the expansion of $\sum_i \prod_{j \neq i} (1 - x_j t)$, every monomial of the form $(-1)^j x_{i_1} x_{i_2} \cdots x_{i_j} t^j$ appears $n-j$ times (once for every index $i \notin \{i_1, i_2, \dots, i_j\}$). Comparing coefficients of like powers of t on both sides gives the required identities. \square

Example A7.2: Computing Characteristic Polynomials. We compute the characteristic polynomial $f(t) = \det(tI - A) \in \mathbb{F}_7[t]$ of the 4×4 matrix

$$A = \begin{bmatrix} 3 & 1 & 4 & 2 \\ 2 & 5 & 5 & 3 \\ 0 & 6 & 3 & 4 \\ 6 & 2 & 1 & 5 \end{bmatrix}$$

over \mathbb{F}_7 which was generated randomly. The coefficients in $f(t) = t^4 - e_1 t^3 + e_2 t^2 - e_3 t + e_4$ are elementary symmetric polynomials in the eigenvalues; and these in turn are expressible in terms of the moments of the spectrum, these being just the traces $m_k = \text{tr}(A^k) = 4, 2, 1, 3, 4$ for $k = 0, 1, 2, 3, 4$. By Newton's identities we find $e_k = 1, 2, 5, 6, 4$ for $k = 0, 1, 2, 3, 4$, giving $f(t) = t^4 + 5t^3 + 5t^2 + x + 4$. The utility of this approach for determining characteristic polynomials, lies in the simplicity of implementing matrix powers in a variety of computing languages. When working over \mathbb{Q} (or \mathbb{R}), this method requires care due to the growth of matrix entries (or roundoff error); but over a fixed finite field, this is never a concern.

Newton's identities show that the moment polynomials can be recursively expressed as polynomials in e_1, e_2, \dots, e_n with integer coefficients, i.e. $m_k \in \mathbb{Z}[e_1, e_2, \dots, e_n]$ for all $k \geq 0$. A foundational result in classical invariant theory shows that much more generally, *every* symmetric polynomial in x_1, x_2, \dots, x_n is expressible as a polynomial in the elementary symmetric polynomials (with coefficients in F). This says that the subring of $F[x_1, x_2, \dots, x_n]$ consisting of all polynomials invariant under the full symmetric group S_n , is exactly the subring $F[e_1, e_2, \dots, e_n]$. The moment polynomials generate a *subring* of the ring of all symmetric polynomials, i.e. $F[m_1, m_2, \dots, m_n] \subseteq F[e_1, e_2, \dots, e_n]$. In characteristic zero, equality holds as can be seen from Newton's identities; since in characteristic zero we can solve for $e_k = \frac{1}{k} \sum_{i=1}^k (-1)^{i+1} m_i e_{k-i}$ and thereby recursively express e_1, e_2, \dots, e_n in terms of the moment polynomials. Similarly in positive characteristic p , Theorem A7.1 allows us to express the elementary symmetric polynomials e_k in terms of the moments, as long as $k \not\equiv 0 \pmod{p}$.

Although Newton's identities give a very fast and practical recursive method for generating the moment polynomials from the sequence of elementary symmetric polynomials, sometimes it is preferable to have instead a more explicit formula. In such cases we use

Theorem A7.3 (Waring's Formula). For $k \geq 1$, $m_k \in \mathbb{Z}[e_1, e_2, \dots, e_n]$ is given by

$$m_k = \sum_{\substack{i_1, i_2, \dots, i_n \geq 0 \\ i_1 + 2i_2 + 3i_3 + \dots + ni_n = k}} \frac{k(i_1 + i_2 + \dots + i_n - 1)!}{i_1! i_2! \dots i_n!} e_1^{i_1} (-e_2)^{i_2} e_3^{i_3} (-e_4)^{i_4} \dots ((-1)^{n+1} e_n)^{i_n}.$$

Before proving this formula, some remarks bear mention. General results of invariant theory tell us that this expansion is unique (there can be no more than one way to express m_k in terms of the elementary symmetric polynomials since e_1, e_2, \dots, e_n are algebraically independent in $\overline{F}(x_1, x_2, \dots, x_n) \supset \overline{F}$, where \overline{F} is the algebraic closure of F). As indicated already, $m_k \in \mathbb{Z}[e_1, e_2, \dots, e_n]$ as follows by induction using Newton's identities; therefore the coefficients in Waring's Formula must also be integers. Note that Waring's Formula expresses m_k in terms of e_1, e_2, \dots, e_ν only, where $\nu = \min\{k, n\}$; this is because $e_j = 0$ for $j > n$, and the constraints on the indices i_1, i_2, \dots, i_n implicitly require that $i_j = 0$ whenever $j > k$; moreover $i_k \in \{0, 1\}$, and the only term with $i_k = 1$ is $(-1)^{k+1} k e_k$. This yields the following, which we use in Section 16:

Corollary A7.4. For all $k \geq 1$, $m_k + (-1)^k k e_k \in \mathbb{Z}[e_1, e_2, \dots, e_{k-1}]$.

It is not too hard to infer this result directly from Newton's identities. Of course when $k > n$, Corollary A7.4 reduces to the statement $m_k \in \mathbb{Z}[e_1, e_2, \dots, e_n]$ which we have already seen.

Proof of Theorem A7.3. Reversing the list of coefficients in $f(t)$ gives the identity

$$\prod_{i=1}^n (1 - x_i t) = 1 - e_1 t + e_2 t^2 - \dots + (-1)^n e_n t^n$$

in $\mathbb{Z}[x_1, \dots, x_n, t]$. Now in $\mathbb{Q}((x_1, x_2, \dots, x_n, t))$ we obtain the identity

$$\begin{aligned} \sum_{j=1}^{\infty} \frac{m_j}{j} t^j &= \sum_{i=1}^n \sum_{j=1}^{\infty} \frac{x_i^j}{j} t^j = - \sum_{i=1}^n \ln(1 - x_i t) \\ &= - \ln(1 - e_1 t + e_2 t^2 - \dots + (-1)^n e_n t^n) \\ &= \sum_{k=1}^{\infty} \frac{(e_1 t - e_2 t^2 + e_3 t^3 - \dots + (-1)^{n+1} e_n t^n)^k}{k} \\ &= \sum_{i_1, i_2, \dots, i_n \geq 0} \binom{i_1 + i_2 + \dots + i_n}{i_1, i_2, \dots, i_n} e_1^{i_1} (-e_2)^{i_2} e_3^{i_3} \dots ((-1)^{n+1} e_n)^{i_n} \frac{t^{i_1 + 2i_2 + 3i_3 + \dots + ni_n}}{i_1 + i_2 + \dots + i_n}. \end{aligned}$$

Comparing coefficients of t^k on both sides gives Waring's formula. \square

Appendix A8: Computational Software

Listed below are six reputable software packages of use in computational algebra. Of these, the first two (PARI/GP and Mathematica) are probably your best options for this course. We have attached sample worksheets for both of these, demonstrating worked examples taken from these notes.

PARI/GP

PARI is open source software designed specifically for computational number theory. Although it is not a general purpose package for symbolic computation, for computational number theory its capabilities are on par with anything else you will have access to; and it is easier to install than any of the other systems. It is freely available for download in Windows, Mac and Linux versions, from

<https://pari.math.u-bordeaux.fr/download.html>

In addition to the documentation available through the official PARI/GP website, many tutorials are available online in both video and readable document form.

Mathematica

Although Mathematica is proprietary software, it is accessible to current students through our campus license. It is suitable for general symbolic computation, not only in computational number theory, but for a wide range of mathematical tasks.

Maple

Another general purpose package for symbolic computation, including computational number theory, is Maple. This is proprietary software which is also currently available to our students; but we anticipate losing the license for this about a year from now.

Sage

Sage is open source software for performing general symbolic computation. It is freely available for download from

<http://www.sagemath.org/download.html>

although trickier to install and use than other options. It is also not as full-featured as the other software available; but it is steadily growing thanks to the programming contributions of its devoted users and fans.

GAP (Groups, Algorithms and Programming)

GAP is open source software which excels at some kinds algebraic symbolic computation. It is intended primarily for group theory, but it offers some more general functionality as well. It is not too hard to install, and it is freely available for download from

<https://www.gap-system.org/>

Magma

Magma is proprietary software for general algebraic computation. However if you are interested, you might ask around our department for help getting this installed.

PARI/GP

The screenshot below (on the right) shows a short PARI/GP session verifying selected details from our Example A3.13. Ending a command with a semicolon suppresses output. This interactive session included 16 input commands. Our comments on the session, as follows, are listed according to step numbers:

- | | |
|---|---|
| <p>[1] Input the minimal polynomial $f(x) = x^4 - x + 3$.</p> <p>[2] We compute the discriminant to be 6885.</p> <p>[3] We factor the discriminant as $3^4 \cdot 5 \cdot 17$.</p> <p>[4] The ideal $(2) \subset \mathbb{Z}$ remains prime in the extension (just one prime factor $2\mathcal{O}$).</p> <p>[5] Compute the ramification index $e = 1$, residual degree $f = 4$, and generator 2 of $2\mathcal{O}$.</p> <p>[6] Find that $3\mathcal{O}$ has two distinct prime factors.</p> <p>[7] The first prime factor of $3\mathcal{O}$ is $(3, -1 + \theta)$ with $e = 3$, $f = 1$.</p> <p>[8] The second prime factor of $3\mathcal{O}$ is $(3, \theta)$ with $e = 1$, $f = 1$.</p> <p>[9] Find that $17\mathcal{O}$ has three distinct prime factors.</p> <p>[10] The first prime factor of $17\mathcal{O}$ is $(17, -7 + \theta)$ with $e = 1$, $f = 1$.</p> <p>[11] The second prime factor of $17\mathcal{O}$ is $(17, -4 + \theta)$ with $e = 2$, $f = 1$.</p> <p>[12] The third prime factor of $17\mathcal{O}$ is $(17, -2 + \theta)$ with $e = 1$, $f = 1$.</p> <p>[14] The class number is 1 (so \mathcal{O} is a PID).</p> <p>[15] The group of roots of unity has order 2, generated by -1.</p> <p>[16] A fundamental unit is $\theta^3 - \theta^2 + 1$.</p> | <pre>(22:41) gp > f=x^4-x+3 %1 = x^4 - x + 3 (22:41) gp > nf=nfinit(f); nf.disc %2 = 6885 (22:41) gp > factor(%) %3 = [3 4] [5 1] [17 1] (22:41) gp > P2=idealprimedec(nf,2); #P2 %4 = 1 (22:41) gp > [P2[1].e, P2[1].f, P2[1].gen] %5 = [1, 4, [2, [2, 0, 0, 0]~]] (22:41) gp > P3=idealprimedec(nf,3); #P3 %6 = 2 (22:41) gp > [P3[1].e, P3[1].f, P3[1].gen] %7 = [3, 1, [3, [-1, 1, 0, 0]~]] (22:41) gp > [P3[2].e, P3[2].f, P3[2].gen] %8 = [1, 1, [3, [0, 1, 0, 0]~]] (22:41) gp > P17=idealprimedec(nf,17); #P17 %9 = 3 (22:41) gp > [P17[1].e, P17[1].f, P17[1].gen] %10 = [1, 1, [17, [-7, 1, 0, 0]~]] (22:41) gp > [P17[2].e, P17[2].f, P17[2].gen] %11 = [2, 1, [17, [-4, 1, 0, 0]~]] (22:41) gp > [P17[3].e, P17[3].f, P17[3].gen] %12 = [1, 1, [17, [-2, 1, 0, 0]~]] (22:41) gp > bnf=bnfinit(nf); (22:41) gp > bnf.no %14 = 1 (22:41) gp > bnf.tu %15 = [2, Mod(-1, x^4 - x + 3)] (22:41) gp > bnf.fu %16 = [Mod(x^3 - x^2 + 1, x^4 - x + 3)] (22:41) gp > ■</pre> |
|---|---|

In fact, the default command for computing the class number in PARI/GP is conditional on GRH (the Generalized Riemann Hypothesis). Should you choose not to trust this result, the PARI/GP documentation describes how to verify this computation unconditionally (i.e. without relying on GRH).

Mathematica

The following pages show a Mathematica session checking some of the steps in the same Example A3.13. Although Mathematica does not currently have all features available, you will have no trouble reproducing all the details of Example A3.13 using Mathematica to do the laborious calculation, if you know what you are doing and follow the steps shown in our worked Example A3.13.

Example A3.13: A Quartic Extension

In[3]:= $f = x^4 - x + 3$

Out[3]= $3 - x + x^4$

In[4]:= $\theta = \text{Root}[f, 1]$

Out[4]= $\text{Root}[3 - \theta + \theta^4, 1]$

Compute the discriminant and its factorization

In[5]:= $\text{NumberFieldDiscriminant}[\theta]$

Out[5]= 6885

In[6]:= $\text{FactorInteger}[\%]$

Out[6]= $\{\{3, 4\}, \{5, 1\}, \{17, 1\}\}$

Verify irreducibility

In[*]:= $\text{Factor}[f]$

Out[*]= $3 - x + x^4$

Factor $f(x)$ over small primes

In[*]:= $\text{Factor}[f, \text{Modulus} \rightarrow 2]$

Out[*]= $1 + x + x^4$

In[*]:= $\text{Factor}[f, \text{Modulus} \rightarrow 3]$

Out[*]= $x(2 + x)^3$

In[*]:= $\text{Factor}[f, \text{Modulus} \rightarrow 5]$

Out[*]= $(1 + x)^2(3 + 3x + x^2)$

In[*]:= $\text{Factor}[f, \text{Modulus} \rightarrow 7]$

Out[*]= $(2 + x)(5 + 4x + 5x^2 + x^3)$

In[*]:= $\text{Factor}[f, \text{Modulus} \rightarrow 11]$

Out[*]= $3 + 10x + x^4$

In[*]:= $\text{Factor}[f, \text{Modulus} \rightarrow 13]$

Out[*]= $3 + 12x + x^4$

In[6]:= **Factor[f, Modulus → 17]**

Out[6]= $(10 + x) (13 + x)^2 (15 + x)$

In[6]:= **Factor[f, Modulus → 19]**

Out[6]= $(10 + x) (6 + 5x + 9x^2 + x^3)$

In[6]:= **Factor[f, Modulus → 23]**

Out[6]= $(14 + x) (15 + 12x + 9x^2 + x^3)$

In[6]:= **Factor[f, Modulus → 29]**

Out[6]= $(3 + x) (6 + x) (5 + 20x + x^2)$

Compute Roots of Unity

In[7]:= **NumberFieldRootsOfUnity[theta]**

Out[7]= $\{-1, 1\}$


Compute Fundamental Units

In[8]:= **NumberFieldFundamentalUnits[theta]**

Out[8]= $\{\text{AlgebraicNumber}[\text{Root}[3 - \sqrt{1} + \sqrt{1^4} \&, 1], \{-1, 0, 1, -1\}]\}$

Compute Class Number

In[9]:= **NumberFieldClassNumber[theta]**

 **NumberFieldClassNumber**: The class number of the number field generated by $\text{Root}[3 - \sqrt{1} + \sqrt{1^4} \&, 1, 0]$ is not yet available.

Out[9]= **NumberFieldClassNumber** $[\text{Root}[3 - \sqrt{1} + \sqrt{1^4} \&, 1]]$

Bibliography

- [ACD] R.J.R. Abel, C.J. Colbourn and J.H. Dinitz, ‘Mutually orthogonal latin squares’, pp.160–193 in *Handbook of Combinatorial Designs, 2nd ed.*, ed. C.J. Colbourn and J.H. Dinitz, Chapman & Hall/CRC, Boca Raton, 2007.
- [Ar] E. Artin, *Galois Theory*, 2nd ed., Univ. Notre Dame, 1944.
- [AK] E.F. Assmus, Jr. and J.D. Key, ‘Hadamard matrices and their designs: a coding-theoretic approach’, *Trans. Amer. Math. Soc.* **330** no.1 (1992), 269–293.
- [AS] E.F. Assmus, Jr. and C.J. Salwach, ‘The $(16, 6, 2)$ designs’, *Internat. J. Math. and Math. Sci.* **2** no.2 (1979), 261–281.
- [BH] L.D. Baumert and M. Hall, Jr., ‘Hadamard matrices of the Williamson type’, *Math. Comp.* **19** no.91 (1965), 442–447.
- [Bl] A. Blokhuis, ‘Polynomials in finite geometries and combinatorics’, pp.35–52 in: *Surveys in Combinatorics, 1993*, ed. K. Walker, Camb. Univ. Press, 1993.
- [BD] T. Bröcker and T. tom Dieck, *Representations of Compact Lie Groups*, Springer, New York, 1985.
- [BR] R.H. Bruck and H.J. Ryser, ‘The nonexistence of certain finite projective planes’, *Canad. J. Math.* **1** (1949) 88–93.
- [Ca] S. Cavior, ‘Exponential sums related to polynomials over $GF(p)$ ’, *Proc. Amer. Math. Soc.* **15** (1964), 175–178.
- [CR] S. Chowla and H.J. Ryser, ‘Combinatorial problems’, *Canad. J. Math.* **2** (1950), 93–99.
- [CM] R. Coulter and R.W. Matthews, ‘Planar functions and planes of Lenz-Barlotti class II’, *Des. Codes Crypt.* **10** (1977) 167–184.
- [DO] P. Dembowski and T.G. Ostrom, ‘Planes of order n with collineation groups of order n^2 ’, *Math. Z.* **103** (1968) 239–258.
- [Ga] D.J.H. Garling, *A Course in Galois Theory*, Camb. Univ. Press, Cambridge, 1986.
- [Gl] D. Gluck, ‘A note on permutation polynomials and finite geometries’, *Discrete Math.* **80** (1990) 97–100.
- [Hp] U. Haagerup, ‘Orthogonal maximal $*$ -subalgebras of the $n \times n$ matrices and cyclic n -roots’, pp.296–322 in *Operator Algebras and Quantum Field Theory (Rome)*, International Press, Cambridge MA, 1996.
- [Ha] M. Hall, Jr., ‘A survey of difference sets’, *Proc. Amer. Math. Soc.* **7** (1956) 975–986.
- [HR] M. Hall, Jr. and H.J. Ryser, ‘Cyclic incidence matrices’, *Can. J. Math.* **3** (1951) 495–502.
- [HH] B. Hartley and T.O. Hawkes, *Rings, Modules and Linear Algebra*, Camb. Univ. Press, Cambridge, 1970.

- [Hi] Y. Hiramane, ‘A conjecture on affine planes of prime order’, *J. Combin. Theory Ser. A* **52** (1989) no. 1, 44–50.
- [Ho] S.F. Hobbs, ‘The law which is not yet in the law books, yet fills them’, pp.93–101 in *Alabama State Bar Association: Report of the Proceedings of the Annual Meeting, July 1st and 2nd, 1926*’.
- [HP] D.R. Hughes and F.C. Piper, *Projective Planes*, Springer Verlag, New York, 1973.
- [Is] I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press, San Diego, 1976.
- [IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, New York, 1990.
- [Ju] D. Jungnickel, ‘Difference sets’, pp.241–324 in *Contemporary Design Theory: A Collection of Surveys*, ed. J.H. Dinitz and D.R. Stinson, Wiley, New York, 1992.
- [JS1] D. Jungnickel and B. Schmidt, ‘Difference sets: an update’, pp.89–112 in *Geometry, Combinatorial Designs and Related Structures: Proceedings of the First Pythagorean Conference*, ed. J.W.P. Hirschfeld, S.S. Magliveras and M.J. de Resmini, Camb. Univ. Press, Cambridge, 1997.
- [JS2] D. Jungnickel and B. Schmidt, ‘Difference sets: a second update’, *Rend. Circ. Palermo Serie II, Suppl.* **53** (1998) 89–118.
- [K] N.M. Katz, ‘An overview of Deligne’s proof of the Riemann hypothesis for varieties over finite fields’, *Proc. Symp. Pure Math.* **28**, Amer. Math. Soc., Providence, R.I., 1976, pp.275–305.
- [Ki] R.E. Kibler, ‘A summary of noncyclic difference sets, $k < 20$ ’, *J. Comb. Theory* **25** (1978), 62–67.
- [L1] S. Lang, *Cyclotomic Fields I and II: Combined Second Edition*, Springer, New York, 1990.
- [L2] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer-Verlag, New York, 1994.
- [LN] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, ed. G.-C. Rota, Camb. Univ. Press, Cambridge, 1997.
- [LeS] K.H. Leung and B. Schmidt, ‘New restrictions on possible orders of circulant Hadamard matrices’, *Des. Codes Cryptogr.* **64** (2012), 143–151.
- [LoS] L. Lovász and A. Schrijver, ‘Remarks on a theorem of Rédei’, *Studia Scient. Math. Hungar.* **16** (1981), 449–454.
- [MM] D.P. May and G.E. Moorhouse, ‘Uniqueness of mutually unbiased bases of order 5’, preprint, 2009.
- [Mc] P.J. McCarthy, *Algebraic Extensions of Fields*, Dover, New York, 1991.
- [M1] G.E. Moorhouse, ‘Bruck nets, codes, and characters of loops’, *Des. Codes Crypt.* **1** (1991), 7–29.

- [M2] G.E. Moorhouse, *Abstract Algebra I*, University of Wyoming, revised 2003.
<http://ericmoorhouse.org/handouts/algebra.pdf>
- [M3] G.E. Moorhouse, *Incidence Geometry*, revised 2017.
http://ericmoorhouse.org/handouts/Incidence_Geometry.pdf
- [M4] G.E. Moorhouse, ‘Codes of nets and projective planes’, pp. 207–216 in: *Error-Correcting Codes, Finite Geometries and Cryptography*, ed. A.A. Bruen and D.L. Wehlau, Contemporary Mathematics **523**, American Mathematical Society, Providence RI, 2010.
- [MSW] G.E. Moorhouse, S. Sun and J. Williford, ‘The eigenvalues of the graphs $D(4, q)$ ’, *J. Comb. Theory Ser. B* **17** (2017) 1–20.
- [Re] L. Rédei, *Lückenhavte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel, 1970.
- [RS] L.Rónyai and T. Szőnyi, ‘Planar functions over finite fields’, *Combinatorica* **9** (1989) no. 3, 315–320.
- [Ro] M. Rosen, *Number Theory in Function Fields*, Springer, New York, 2002.
- [Sa] P. Samuel, *Algebraic Theory of Numbers*, Dover, Mineola, NY, 1970.
- [S1] B. Schmidt, ‘Cyclotomic integers and finite geometry’, *J. Amer. Math. Soc.* **12** no. 4 (1999) 929–952.
- [S2] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, Springer, Berlin, 2002.
- [Sc] W.M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Springer-Verlag, Berlin, 1976.
- [Se] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.
- [SS] R.G. Stanton and D.A. Sprott, ‘A family of difference sets’, *Canad. J. Math.* **10** (1958) 73–77.
- [Wa] L.C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer Verlag, 1997.
- [Wh] A.L. Whiteman, ‘An infinite family of Hadamard matrices of Williamson type’, *J. Comb. Theory Ser. A* **14** (1973) 334–340.
- [Wi] J. Williamson, ‘Hadamard’s determinant theorem and the sum of four squares’, *Duke J. Math.* **11** (1944) 65–81.

Index

adjacency operator	41	Hadamard	66
affine plane	104	Menon	73
classical (desarguesian)	104, 110	Singer	63
alphabet	42	symmetric	55
algebraic		difference set	54, 63
closure	131	abelian	55
conjugate	153	complementary	63
extension	131	cyclic	55
integer	139	Hadamard	73
number	131, 138	Menon	73
algebraically closed	131	nonabelian	55
antiautomorphism	55	order	56
associate	142	Paley	63
automorphism		parameters	55
of a design	57	Dirichlet's Theorem	
of a field	153, 154	on primes in arithmetic progression	164
regular	57	on units	141
Bernoulli number	34	discriminant	141
block	55	domain	
categorification	6	Dedekind	163
Cavior's Theorem	99	Euclidean (ED)	142, 145
Cayley (di)graph	40	integral (ID)	49
character	36	principal ideal (PID)	142
additive	84	unique factorization (UFD)	142
Dirichlet	164	dual code	43
linear	36	dual group	36
multiplicative	84	dual numbers, ring of	145
order of	85	Eisenstein Criterion	137
principal	36	Eisenstein integers	146
quadratic	9	elementary symmetric polynomial	167
table	117	embedding	150
trivial	9	equivalence	
characteristic of a field	130	of complex Hadamard matrices	117
class number	147	of difference sets	58
code	41	of Hadamard matrices	65
codeword	41	of ideals	147
completely multiplicative function	2, 164	of sets of MUBs	119
complex Hadamard matrix	116	error syndrome	42
normalized	122	Euclidean ring	142, 145
convolution	38, 49	Euler Criterion	77
cyclic group	1	Euler factorization	91, 92, 163, 164
cyclotomic		exponent of a group	36, 147
field	19	exponential sum	96
integer	27	extension	129
number	27	abelian	19
polynomial	5	algebraic	130
unit	27	cubic	148, 156
Dedekind domain	163	cyclic	155
Dedekind zeta function	163	degree of	129
design		finite	129
automorphism	57	Galois	155
		imaginary quadratic	141
		normal	148

- quadratic 129, 155
- quartic 144
- real quadratic 141
- separable 141
- simple 152, 153
- feasibility relation 55
- Fermat's
 - Last Theorem 29
 - Little Theorem 77
 - method of descent 29, 88
- field 129
 - algebraically closed 131
 - characteristic of 130
 - cyclotomic 19
 - finite 7
 - fixed 157
 - prime 130
 - of rational functions 129
 - splitting 148
- flat 117
- Fourier transform 39
 - discrete (DFT) 44
 - fast (FFT) 44
 - residual 91
- function
 - L - 92, 164
 - multiplicative 2
 - planar 104
 - polynomial 13
 - totient 1
- Galois
 - closure 156
 - correspondence 157
 - group 155
 - theory, Fundamental Theorem of 158
- Gauss sum 85
 - quadratic 79, 95
- Gaussian integers 146
- general linear group 8
- group
 - additive 51
 - algebra 38, 49
 - automorphism 153
 - cyclic 1
 - direct product 52
 - elementary abelian 8
 - Galois 155
 - general linear 8
 - multiplier 61
 - regular 57
 - ring 38, 39
- Hadamard 2-design 66
- Hadamard matrix 66
 - complex 116
 - circulant 74
 - regular 73
 - skew-type 66
 - Williamson type 67
- Hall's Multiplier Theorem 60
- Hasse-Davenport relation 95
- Hasse diagram 158
- ideal 143
 - class group 147
 - maximal 143
 - norm of 143
 - prime 143
 - principal 143
 - product of 143
 - sum of 143
- idempotent 40
 - primitive 40
- information rate 42
- integer (algebraic) 139
 - rational 139
 - ring of 140
- integral domain 49
- irreducible 142
- Jacobi sum 86
- Kronecker-Weber Theorem 20
- Lagrange interpolation 14
- Laurent polynomial 52
- Legendre symbol 77
- Lemma of Tangents 17
- L -function 92
- MacWilliams relations 43
- matrix
 - circulant 67
 - complex Hadamard 116
 - flat 117
 - generator 42
 - Gram 117
 - Hadamard 64
 - parity check 42
 - representation 132
 - Vandermonde 15, 22, 45
- migration of units 142
- minimal polynomial 130
- moment polynomial 167
- monic 8
- monomial

- equivalence 65, 119
- unitary matrix 119
- monomorphism 150
- multiplicative function 2
- multiplier 61, 63
 - Conjecture 61
 - group 61
- mutually unbiased 118
- MUBs 119
 - complete set of 120
- net 107
 - classical (desarguesian) 111
 - cyclic 111
- Newton's identities 167
- nonsquare 10, 77
- norm
 - absolute 132
 - of an element 132, 159
 - of an ideal 91, 143
- normal closure 148, 156
- normal basis 160
- number field 140
- order of a character 85
- order of a design 56, 104, 107
- Paley 66
- parallel 104, 108
- passant 101
- perfect 4
- planar function 104
- plane
 - affine 104
 - projective 56
- point 55
- polynomial function 13
- power sum polynomial 167
- prime
 - ideal 143
 - irregular 34
 - Mersenne 4
 - ramifies 144
 - regular 34
 - Sophie Germain pair 35
 - splits 144
 - subfield 130
- primitive
 - element 151
 - idempotent 40
 - root of unity 1, 4
- projective plane 56
 - classical (desarguesian) 63
- quadratic
 - character 9
 - extension 129, 155
 - Gauss sum 79, 95
 - reciprocity 77
- ramification 144
- reducible 142
- regular permutation group 57, 154
- representation theory 40
- residual degree 144
- residual field 91
- root lattice 76
- secant 101
- Segre's Theorem 16
- sharply divides 35
- splitting field 148
- spectrum 41
- square 10, 77
- squarefree 3
- Streetlight Effect 64
- subfield
 - fixed 157
 - intermediate 157
 - maximal real 23
 - prime 130
- subnet 110
- symmetric polynomial 159, 167
 - elementary 167
 - power sum (moment) 167
- tangent 16, 101
- totient function 1
- tower of fields 129
- trace 132, 159
 - absolute 132
- transitivity
 - of extension degree 129
 - of norm and trace 134
- twin prime power 66
- unbiased 118
- unique factorization 142
- unit 141
- Vandermonde matrix 15, 22, 45
- Waring's Formula 169
- weight
 - distribution 41
 - enumerator 43
 - minimum 41
 - of a vector 41
 - of a polynomial 136
- Weil's bound 97
- Wilson's Theorem 18
- word 41
- zeta function 91
 - Dedekind 163
 - Riemann 91, 163