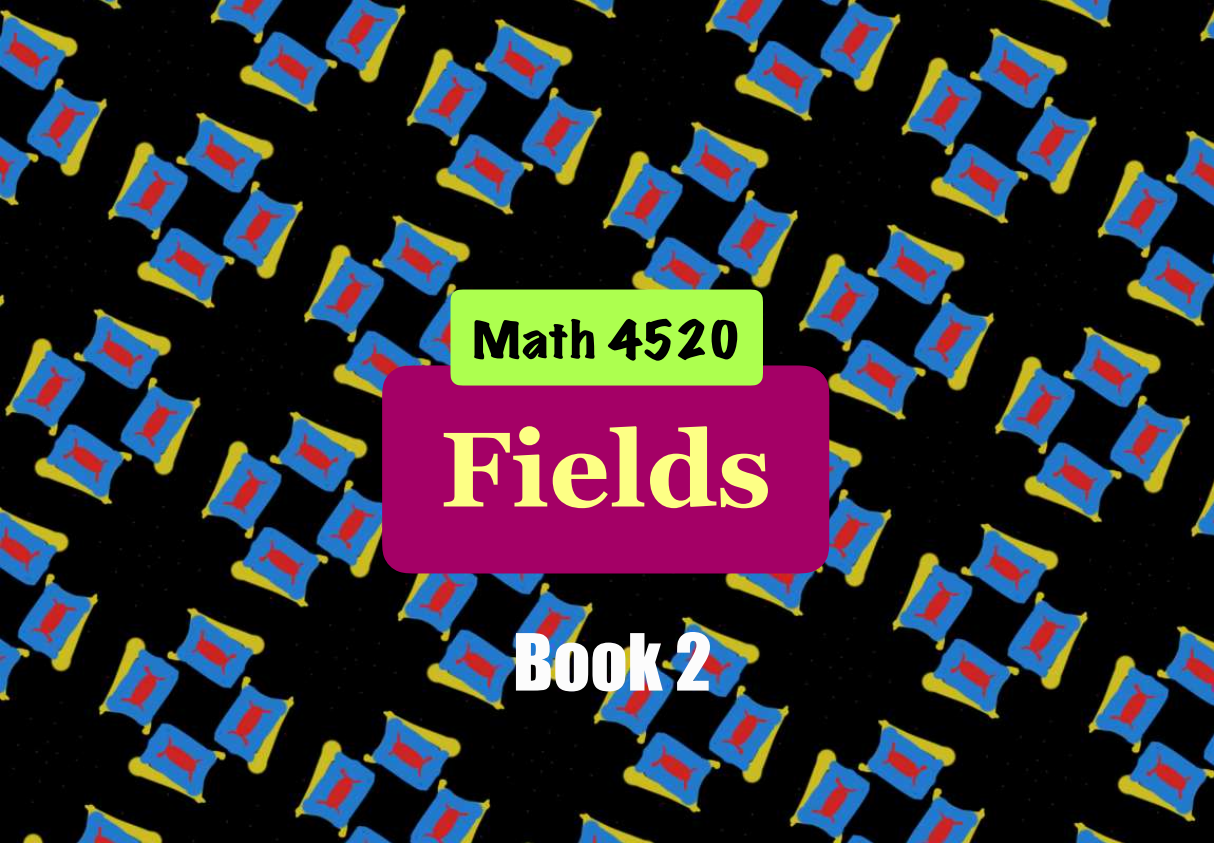




Math 4520

Fields

Book 2

Polynomials over $\mathbb{F}_2 = \{0, 1\} = F$ the field of order 2

There are 2^n polynomials of degree n over $\mathbb{F}_2$:

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, \quad a_0, \dots, a_{n-1} \in \mathbb{F}_2$$

(necessarily monic).

Polynomials $f(x) \in F[x]$

Degree 1: $x, x+1$ are both irreducible

Degree 2: $x^2, x^2+1, x^2+x, x^2+x+1$
 $\underbrace{x^2}_{x \cdot x} \quad \underbrace{(x+1)^2}_{(x+1)(x+1)} \quad \underbrace{x(x+1)}_{x(x+1)} \quad \text{irreducible}$
 $\underbrace{= (x+1)(x+1)}_{\text{reducible}}$

Degree 3: $x^3 + ax^2 + bx + c, \quad a, b, c \in F$

Reducible: $x^3 = x \cdot x \cdot x$
 $x^3 + x^2 = x \cdot x \cdot (x+1)$
 $x^3 + x = x \cdot (x+1) \cdot (x+1)$
 $x^3 + x^2 + x + 1 = (x+1) \cdot \underbrace{(x+1)(x+1)}_{x^2+1}$
 $x^3 + x^2 + x = x(x^2 + x + 1)$
 $x^3 + 1 = (x+1)(x^2 + x + 1)$

Irreducible: $x^3 + x + 1, x^3 + x^2 + 1$

Degree 4: $x(x^3 + x + 1) = x^4 + x^2 + x$
 $(x+1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$
 $x(x^3 + x^2 + 1) = x^4 + x^3 + x$
 $(x+1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$
 $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1$
 $x^2(x^2 + x + 1) = x^4 + x^3 + x^2$
 $(x^2 + 1)(x^2 + x + 1) = x^4 + x^3 + x + 1$
 $(x^2 + x)(x^2 + x + 1) = x^4 + x$
 $x^3(x+1) = x^4 + x^3$
 $x^2(x+1)^2 = x^4 + x^2$
 $x(x+1)^3 = x^4 + x^3 + x^2 + x$
 $(x+1)^4 = x^4 + 1$

reducible

irreducible
 $x^4 + x^3 + x^2 + x + 1$
 $x^4 + x + 1$
 $x^4 + x^3 + 1$

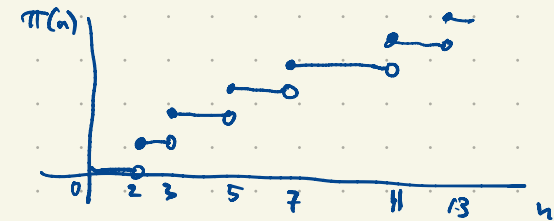
Given prime p , and integer $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

In fact we can count the number of irreducible polynomials of each degree.

$\mathbb{Z}$ and $\mathbb{F}_p[x]$ are two rings which are commutative rings with identity having unique factorization into irreducible factors. They are both Euclidean domains (having Division Algorithm and Euclidean algorithm).

There are roughly $\frac{n}{\ln n}$ prime numbers less than n for large n .

$\pi(n)$ = number of primes $\leq n$.
 $\pi(10) = 4, \pi(11) = 5$.



$$\pi(n) \sim \frac{n}{\ln n}$$

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln n} = 1$$

Prime Number Theorem
 Gauss conjectured this formula.

In $F[x]$, $F = \mathbb{F}_2 = \{0, 1\}$, the polynomial $x^2 + x + 1 \in F[x]$ is irreducible.
 The extension $E = F(\alpha) = \{a + b\alpha : a, b \in F\}$ is an extension field i.e. $F \subseteq E$ is a subfield.
 $= \{0, 1, \alpha, \underbrace{\alpha+1}_{\beta}\}$ This is the field of order 4 found previously.
 $\alpha^2 + \underbrace{\alpha+1}_{\beta} = 0 \Rightarrow \alpha^2 = -\beta = \beta$

Eg. field of order 8. $m(x) = x^3 + x + 1 \in F[x]$, $F = \mathbb{F}_2 = \{0, 1\}$. $m(x)$ is irreducible in $F[x]$.
 Declare α to be a root of $m(x)$ in $E \supset F$, an extension field. $m(0) = m(1) = 1$ so m has no roots in F .

$$E = \{a + b\alpha + c\alpha^2 : a, b, c \in F\}$$

$$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

$$= \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$$

$$\beta = \alpha^2 + 1 = \alpha^6$$

$$\gamma = \alpha^2 + \alpha + 1 = \alpha^5$$

$$\beta + \gamma = (\alpha^2 + 1) + (\alpha^2 + \alpha + 1) = \alpha$$

$$\beta\gamma = (\alpha^2 + 1)(\alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha + 1 = (\alpha + \alpha^2) + (\alpha + 1) + \alpha + 1 = \alpha^2 + \alpha$$

$$\beta\gamma = \alpha^6 \alpha^5 = \alpha^{11} = \alpha^4 = \alpha^2 + \alpha$$

$$m(\alpha) = \alpha^3 + \alpha + 1 = 0 \Rightarrow$$

$$\alpha^3 = -1 - \alpha = 1 + \alpha$$

$$\alpha^4 = \alpha + \alpha^2$$

$$\alpha^5 = \alpha^2 + \alpha^3 = \alpha^2 + (\alpha + 1) = \alpha^2 + \alpha + 1$$

$$\alpha^6 = \alpha^3 + \alpha^2 + \alpha = (\alpha + 1) + \alpha^2 + \alpha = \alpha^2 + 1$$

$$\alpha^7 = \alpha^3 + \alpha = (\alpha + 1) + \alpha = 1$$

Adding elements of E is easier using the first description $E = \{a + b\alpha + c\alpha^2 : a, b, c \in F\}$.

Multiplying elements of E is easier using the second description $E = \{0, 1, \alpha, \alpha^2, \dots, \alpha^6\}$.

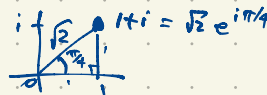
$$\text{Compare: } \mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} = \{re^{i\theta} : r, \theta \in \mathbb{R}\}$$

Addition in $\mathbb{C}$ is easier in rectangular form e.g. $(5 + 3i) + (7 - 11i) = 12 - 8i$

Multiplication in $\mathbb{C}$ ----- polar form $(re^{i\theta})(se^{i\phi}) = rs e^{i(\theta+\phi)}$

$$(1+i)^{37} = (1+i)(1+i)(1+i)\dots(1+i) = (\sqrt{2} e^{i\pi/4})^{37} = \sqrt{2}^{37} \cdot e^{(i\pi/4)37} = 262144\sqrt{2} \left(-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i\right)$$

$$= -262144 - 262144i$$



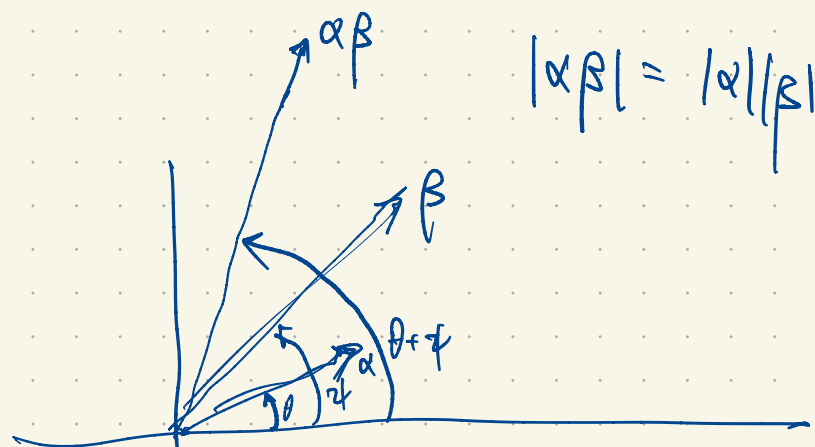
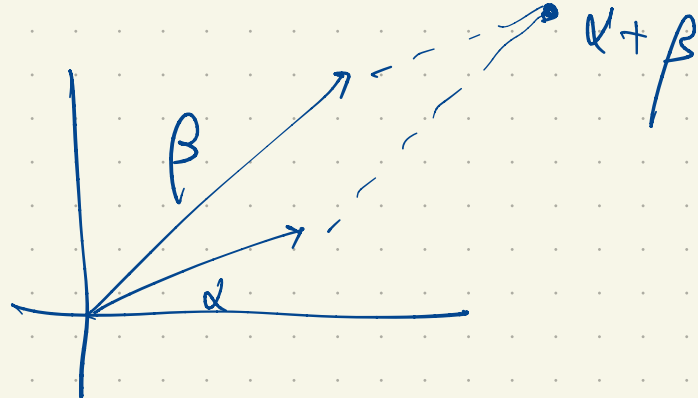
$$\sqrt{2} = 2^{1/2}$$

$$\sqrt{2}^{37} = 2^{37/2} = 2^{18} \sqrt{2}$$

$$\frac{1024}{256}$$

$$e^{i\pi/4 \cdot 37} = e^{i\pi/4 \cdot 37} = 262144\sqrt{2}$$

$$= e^{8\pi i} \cdot e^{5\pi/4 i} \quad \frac{37}{4} = 9\frac{1}{4}$$



In any finite field, the nonzero elements form a cyclic group i.e. they are all powers of a single element called a primitive element.

Field of order 16: $m(x) = x^4 + x + 1 \in F[x]$ is irreducible, $F = \{0, 1\} = \mathbb{F}_2$.

Let α be a root of $m(x)$ i.e. $\alpha^4 + \alpha + 1 = 0$ i.e. $\alpha^4 = \alpha + 1$.

$E = \{a + b\alpha + c\alpha^2 + d\alpha^3 : a, b, c, d \in F\}$, $|E| = 2^4 = 16$.

$= \{0, 1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{14}\}$, $\alpha^{15} = 1$. α is primitive.

$$\begin{aligned} \alpha^4 &= \alpha + 1 \\ \alpha^5 &= \alpha^2 + \alpha \end{aligned}$$

If F is any field then $F^* = \{\text{nonzero elements in } F\}$ is an abelian (multiplicative) group.

If R is any ring with identity then $R^* = \{\text{units in } R\}$ is a group.

eg. $R = \{n \times n \text{ matrices over } R\}$ then $R^* = GL_n(R) = \{\text{invertible } n \times n \text{ matrices over } R\}$

If R is a commutative ring with identity then R^* is an abelian group.

eg. $R = \mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, \dots, 11\}$ with addition and multiplication mod 12.

If $R = \mathbb{Z}/10\mathbb{Z} = \{0, 1, 2, \dots, 9\}$ mod 10

$R^* = \{1, 5, 7, 11\}$

$x^2 - 1 \in R[x]$ has four roots in R .

x	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Klein four-group
(not cyclic)

x	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$R^* = \{1, 3, 7, 9\}$

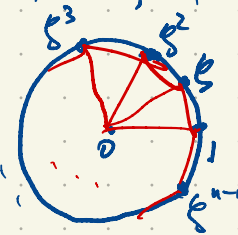
x	1	3	7	9
1	1	3	7	9
3	3	9	7	1
7	7	1	3	9
9	9	7	1	3

cyclic group
of order 4

$\mathbb{C}^* = \{\text{all nonzero complex numbers}\}$

Every finite subgroup of this subgroup is cyclic.

n^{th} roots of unity: solutions of $z^n = 1$
 $\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$ $n \geq 1$, $\zeta = e^{2\pi i/n}$



If F is a finite field then F^* is a cyclic group.

eg. $\mathbb{F}_7 = \{0, 1, 2, \dots, 6\}$, $\mathbb{F}_7^* = \{1, 2, \dots, 6\} = \langle 3 \rangle = \{1, 3, 3^2, 3^3, 3^4, 3^5\}$, $3^6 = 1$

3 is a generator for this cyclic group

eg. $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, $\mathbb{F}_5^* = \{1, 2, 3, 4\}$. This abelian group of order 4 is cyclic which must be cyclic

$$\begin{aligned} 3^0 &= 1 \\ 3^1 &= 3 \\ 3^2 &= 9 = 4 \\ 3^3 &= 27 = 2 \\ 3^4 &= 81 = 1 \end{aligned}$$

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 = 3 \end{aligned}$$

2 is not a generator.
 3 is primitive mod 7,
 2 is not.

x	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Not a Klein four-group

x	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

cyclic group of order 4

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 3 \\ 2^4 &= 1 \end{aligned}$$

Theorem If F is any field then every finite subgroup of F^* is cyclic.

In particular if F is any finite field, then F^* is cyclic.

Idea of proof in the case of $\mathbb{F}_5$, why can't $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ be a Klein four-group?

In a Klein four-group, $x^2 = 1$ for all x . If $\mathbb{F}_5^*$ were a Klein four-group then

$x^2 - 1$ would have four roots 1, 2, 3, 4.

In a field, no polynomial of degree 2 can have four distinct roots.

If $f(x) = x^2 + ax + b$ has roots $r \neq s$ then $f(x) = (x-r)(x-s)$ and r, s are the only roots.

In $\mathbb{F}_{16}$, $\mathbb{F}_{16}^*$ is an abelian group of order 15. Every element has order 1, 3, 5 or 15. If we have an element of order 15 then $\mathbb{F}_{16}^*$ is cyclic. If every element has order 1 or 5 then $x^5 - 1$ would have 15 roots on the field.

In $F[x]$, F a field, every root $r \in F$, $f(r) = 0$ (r root of $f(x)$) $\iff x-r$ is a factor of $f(x)$.
This uses the Division Algorithm. $f(x) = (x-r)q(x) + h(x)$. When r is a root, $h=0$ so $f(x) = (x-r)q(x)$.

If $r_1, \dots, r_n$ are distinct roots then $f(x) = (x-r_1)(x-r_2)\dots(x-r_n)q(x)$
 $\deg h(x) < 1$
 $h = h(x) = \text{constant}$
 $\Rightarrow n \leq \deg f(x)$

Application: to cryptography

eg. $\mathbb{F}_{13} = \{0, 1, 2, \dots, 12\}$

$$\mathbb{F}_{13}^* = \{1, 2, \dots, 12\} = \{2^k : 0 \leq k \leq 11\}$$

2 generates the cyclic group $\mathbb{F}_{13}^*$ of order 12.
We call 2 a primitive element.

$$\text{Solve } 2^x \equiv 9 \pmod{13}.$$

$$x \equiv 8 \pmod{12}.$$

$$x = 12k + 8$$

$$2^x = 2^{12k+8} = (2^{12})^k \cdot 2^8 = 1 \cdot 9 = 9.$$

If p is a large prime then solving

$2^x \equiv a$ for x (when $a \in \mathbb{F}_p^*$ is given)
 or better yet, $g^x = a$ (g is a primitive element)
 is HARD.

Computing 2^x or g^x is EASY.

k	2^k	in $\mathbb{F}_{13}^*$
0	1	
1	2	
2	4	
3	8	
4	3	
5	6	
6	12	
7	11	
8	9	
9	5	
10	10	
11	7	
12	1	

$\gcd(k, 12) = 1$
 $\iff k$ is relatively prime with 12

$\iff k \equiv 1, 5, 7 \text{ or } 11 \pmod{12}$

2, 6, 11, 7 $\in \mathbb{F}_{13}$ are primitive
 (any one of these serves as a generator for $\mathbb{F}_{13}^*$)

	Oct	
M	W	F
26	—	—
	Nov	
2	4	6
		↑
		Test

eg. $p = 17$

$$2^{16} \equiv 1 \pmod{17}$$

(Fermat's Little Theorem or Lagrange's Theorem)

$$2^{19} = ?$$

squaring

$$\begin{aligned} 2^1 &= 2 \\ 2^2 &= 4 \\ 2^4 &= 16 \\ 2^8 &= 256 = 21 \\ 2^{16} &= 111 = 18 \end{aligned}$$

$$2^{19} = 2^{16} \cdot 2^2 \cdot 2^1 = 18 \cdot 4 \cdot 2 = 3.$$

$$2 = 29$$

Solving this is the discrete logarithm problem

In $\mathbb{R}^* = \{\text{nonzero real numbers}\}$ solve $2^x = 29 \iff x = \log_2 29 = \frac{\ln 29}{\ln 2}$

$$\ln 2^x = \ln 29$$

$$x \cdot \ln 2 = \ln 29$$

$$x = \frac{\ln 29}{\ln 2}$$

Diffie-Hellman Key Exchange Protocol

Alice and Bob are able to communicate over an insecure channel (eg. email)

They need to share a secret key eg. (long alphanumeric string).

Alice generates a large prime p . (eg. 250 digits long)

She also chooses a random $g \in \mathbb{F}_p^*$ i.e. $g \in \{1, 2, \dots, p-1\}$.

Alice sends g and p to Bob. (This is safe.)

Alice chooses $a \in \{2, 3, \dots, p-2\}$ randomly and keeps this a secret.

Bob chooses $b \in \{2, 3, \dots, p-2\}$...