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 $\mathbb{F}_2$:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_0, \ldots, a_{n-1} \in \mathbb{F}_2.$$

(necessarily monic).

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

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

Degree 2: $x^2 = x \cdot x$, $x^2+1 = (x+1)^2$, $x^2+x = x(x+1)$, x^2+x+1 irreducible

$= (x+1)(x+1)$ reducible

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

Reducible:

$x^3 = x \cdot x \cdot x$

$x^3 + x^2 = x \cdot x \cdot (x+1)$

$x^3 + x = x \cdot (x+1)(x+1)$

$x^3 + x^2 + x + 1 = (x+1)(x+1)(x+1)$

$x^3 + x^2 + x = x(x^2+x+1)$

$x^3 + 1 = (x+1)(x^2+x+1)$

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

Degree 4:

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

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

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

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

$(x^2+x+1)(x^2+x+1) = x^4 + x^2 + 1$

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

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

$(x^2+x)(x^2+x+1) = x^4 + x$

x^4

$x^3(x+1) = x^4 + x^3$

$x^2(x+1)^2 = x^4 + x^2$

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

$(x+1)^4 = x^4 + 1$

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 $\mathbb{F}_p[x]$.

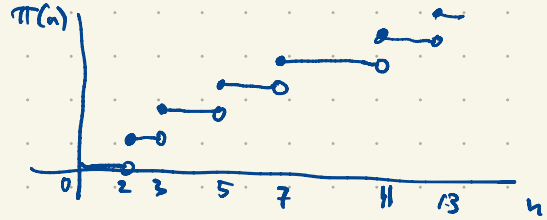
In fact we can count the number of irreducible polynomials of each degree.

$\mathbb{Z}$ 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 $\leq n$.

$\pi(10) = 4$, $\pi(11) = 5$.



$\pi(n) \sim \frac{n}{\ln n}$ Prime number Theorem

Gauss conjectured this formula.

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

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. $F \subset E$ is a subfield.
$= \{0, 1, \alpha, \underbrace{\alpha+1}_{\beta}\}$ This is the field of order 4 found previously.

$$\alpha^2 + \underbrace{\alpha+1}_{\beta} = 0 \Rightarrow \alpha^2 = -\beta = \beta$$

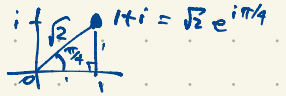
Eg. field of order 8. $m(x) = x^3+x+1 \in F[x]$, $F = \mathbb{F}_2 = \{0,1\}$. $m(x)$ is irreducible in $F[x]$.
Declare α to be a root of $m(x)$ in $E \supset F$, an extension field. $m(0) = m(1) = 1$ so m has no roots in F

$E = \{a+b\alpha+c\alpha^2 : a,b,c \in F\}$
$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$
$= \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$

$m(\alpha) = \alpha^3+\alpha+1 = 0 \Rightarrow \alpha^3 = -1-\alpha = 1+\alpha$
$\alpha^4 = \alpha+\alpha^2$
$\alpha^5 = \alpha^2+\alpha^3 = \alpha^2+(\alpha+1) = \alpha^2+\alpha+1$
$\alpha^6 = \alpha^3+\alpha^2+\alpha = (\alpha+1)+\alpha^2+\alpha = \alpha^2+1$
$\alpha^7 = \alpha^3+\alpha = (\alpha+1)+\alpha = 1$.

$\beta = \alpha^2+1 = \alpha^6$
$\gamma = \alpha^2+\alpha+1 = \alpha^5$
$\beta+\gamma = (\alpha^2+1)+(\alpha^2+\alpha+1) = \alpha$
$\beta\gamma = (\alpha^2+1)(\alpha^2+\alpha+1) = \alpha^4+\alpha^3+\alpha+1 = (\alpha+\alpha^2)+(\alpha+1)+\alpha+1 = \alpha^2+\alpha$
$\beta\gamma = \alpha^6\alpha^5 = \underbrace{\alpha^{11}}_{\alpha^7\cdot\alpha^4} = \alpha^4 = \alpha^2+\alpha$.

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 $E = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$.



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

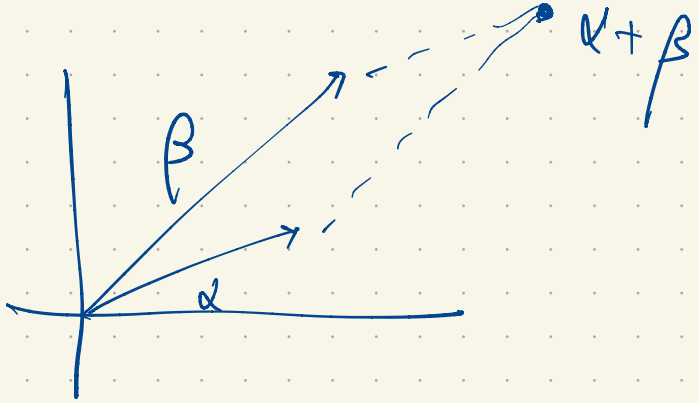
Addition in $\mathbb{C}$ is easier in rectangular form e.g. $(5+3i)+(7-11i) = 12-8i$
Multiplication in $\mathbb{C}$ ---- polar form $(re^{i\theta})(se^{i\phi}) = rs\,e^{i(\theta+\phi)}$

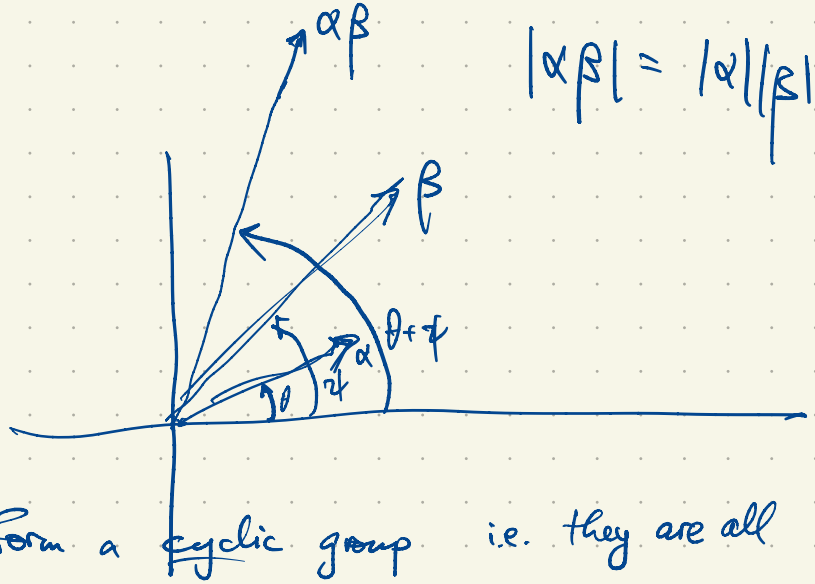


$(1+i)^{37} = (1+i)(1+i)(1+i)\cdots(1+i) = \left(\sqrt{2}\,e^{i\pi/4}\right)^{37} = \sqrt{2}^{37}\cdot e^{(i\pi/4)37} = 262144\sqrt{2}\left(-\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)$
$= -262144 - 262144i$

$\sqrt{2} = 2^{1/2}$
$\sqrt{2}^{37} = 2^{37/2} = 2^{18}\sqrt{2}$ $\quad 1024 \cdot 256$
$= 262144\sqrt{2}$

$e^{i\frac{\pi}{4}\cdot 37} = e^{i\frac{\pi}{4}\cdot 37}$
$= e^{8\pi i}\cdot e^{\frac{5\pi}{4}i}$ $\quad \frac{37}{4} = 9\frac{1}{4}$
$= 1 \cdot \left(-\frac{1}{\sqrt{2}}-\frac{1}{\sqrt{2}}i\right)$





$|\alpha\beta| = |\alpha||\beta|$

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. $\alpha^4 = \alpha + 1$.

$\alpha^4 = \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$

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

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

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

If R is any ring with identity then $R^\times = \{\text{units in } R\}$ is a group.
(invertible elements)

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

If R is a commutative ring with identity then $R^\times$ is an abelian group.

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

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

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

×	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)

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

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

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

×	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

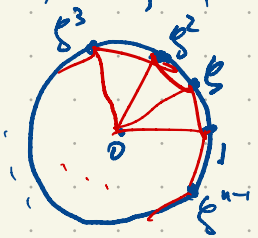
cyclic group of order 4

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

Every finite subgroup of this subgroup is cyclic.

n^{th} roots of unity: solutions of $z^n = 1$

$\{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\}$, $n \geq 1$, $\zeta = e^{2\pi i/n}$



If F is a finite field then $F^\times$ is a cyclic group.

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

3 is a generator for this cyclic group

$3^0 = 1$
$3^1 = 3$
$3^2 = 9 = 2$
$3^3 = 27 = 3$
$3^4 = 81 = 4$
$3^5 = 5$
$3^6 = 1$

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8 = 1$

2 is not a generator.

3 is primitive mod 7, 2 is not.

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

×	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

×	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.

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 3$
$2^4 = 1$

Theorem If F is any field then every finite subgroup of $F^\times$ is cyclic.

In particular if F is any finite field, then $F^\times$ is cyclic.

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

In a Klein four-group, $x^2 = 1$ for all x. If $\mathbb{F}_5^\times$ 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 $f(x) = (x-r)q(x)$.
$\deg h(x) < 1$
$h = h(x) =$ constant

If $r_1, \dots, r_n$ are distinct roots then $f(x) = (x-r_1)(x-r_2)\cdots(x-r_n)q(x) \Rightarrow n \le \deg f(x)$.

Oct

M	W	F
26	—	—
	Nov	
2	4	(6) Test

Application: to cryptography

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

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

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

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

$\gcd(k, 12) = 1$
$\iff$ k is relatively prime with 12
$\iff$ $k \equiv 1, 5, 7$ or $11 \bmod 12$

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

Solve $2^x \equiv 9 \bmod 13$.

$x \equiv 8 \bmod 12$. $\quad x = 12k + 8$

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

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.

eg. $p = 47$

$2^{46} \equiv 1 \bmod 47$ (Fermat's Little Theorem or Lagrange's Theorem)

$2^{19} = ?$

squaring: $2^1 = 2$, $2^2 = 4$, $2^4 = 16$, $2^8 = 256 = 21$, $2^{16} = 441 = 18$

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

$2^? = 29$ 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. $g \in \{1, 2, \cdots, p-1\}$.
Alice sends g and p to Bob. (This is safe.)
Alice chooses $a \in \{2, 3, \cdots, p-2\}$ randomly and keeps this a secret.

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

Alice computes $g^a \bmod p$ (in $\mathbb{F}_p$) and sends it to Bob.
Bob . . $g^b \bmod p$ (in $\mathbb{F}_p$) . . . . . Alice.

Alice computes $(g^b)^a = g^{ab} \bmod p$.
Bob computes $(g^a)^b = g^{ab} \bmod p$.
} This secret value is shared by Alice and Bob.

An eavesdropper knows g, p, g^a, g^b. The eavesdropper does not know a, b, g^{ab}.

g, p, g^a, g^b: integers mod p. g^{ab}: $\mathbb{F}_p$.

How can an eavesdropper figure out $g^{ab} \bmod p$ from g, p, g^a, g^b? If the eavesdropper can figure out a or b then it's easy to get g^{ab}. Is there a shortcut to finding g^{ab} without first finding a or b? Maybe but probably not.

Let F be a field.

$F[x]$ is the ring of all polynomials in x with coefficients in F.

$F[x]$ is an integral domain: commutative ring with identity 1 having no zero divisors.

So we can form the field of quotients $F(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x], \ g(x) \neq 0 \right\}$.

(just like how we construct $\mathbb{Q}$ from $\mathbb{Z}$.)

x is just a symbol, not a number.

$F[[x]] = \{$ all power series in x with coefficients in $F \}$

$= \{ a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots : a_i \in F \}$

$= \left\{ \sum_{n=0}^{\infty} a_n x^n : a_n \in F \right\}$

$F[x] \subset F[[x]]$ subring

$1 + 3x - 5x^2 = 1 + 3x - 5x^2 + 0x^3 + 0x^4 + 0x^5 + \cdots$

$= -5x^2 + 3x + 1$

If $f(x) = 3 + 2x - x^2 - 7x^3 + \cdots$

$g(x) = -1 + x^2 + 11x^3 + \cdots$

$f(x) + g(x) = 2 + 2x + 4x^3 + \cdots$

$f(x) - g(x) = 4 + 2x - 2x^2 - 18x^3 + \cdots$

$f(x)g(x) = (3 + 2x - x^2 - 7x^3 + \cdots)(-1 + x^2 + 11x^3 + \cdots) = -3 - 2x + 4x^2 + 42x^3 + \cdots$

$(1 - x)(1 + x + x^2 + x^3 + \cdots) = 1$

$1 + 2 + 2^2 + 2^4 + 2^5 + 2^6 + \cdots = -1$

$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$

If we allow $f(x) \sum_{n=-\infty}^{\infty} a_n x^n = \cdots + a_{-3}x^{-3} + a_{-2}x^{-2} + a_{-1}x^{-1} + a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$

$g(x) = \cdots + b_{-3}x^{-3} + b_{-2}x^{-2} + b_{-1}x^{-1} + b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots$

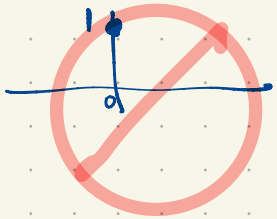
then $f(x)g(x)$ is undefined in general.

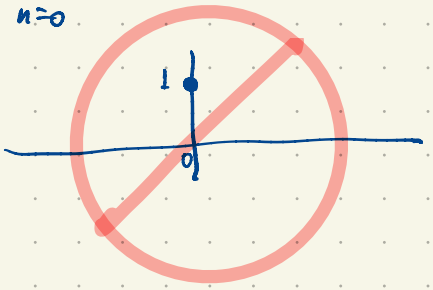
eg. in $\mathbb{R}[[x]]$ consider $f(x) \in \mathbb{R}[[x]]$ defined by $f(x) = 1 + x + 2x^2 + 6x^3 + 24x^4 + 120x^5 + 720x^6 + \cdots$

$$= \sum_{n=0}^{\infty} n!\, x^n .$$

$$f(x)^2 = (1 + x + 2x^2 + 6x^3 + \cdots)(1 + x + 2x^2 + 6x^3 + \cdots)$$

$$= 1 + 2x + 5x^2 + 16x^3 + \cdots$$





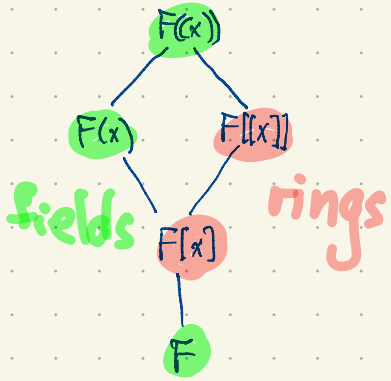
$$(x^{-1} + 1 + x + x^2 + x^3 + \cdots)(x^{-3} + 2x^{-2} - x^{-1} - 1 + 2x + 3x^2 + \cdots) = x^{-4} + 3x^{-3} + x^{-2} + x^{-1} + 3 + (*)x + (*)x^2 + \cdots$$

$F[[x]]$ is contained in a larger ring

$F((x)) = \{$ series in x allowing only finitely terms with negative exponent $\}$

$$= \left\{ \sum_{n=m}^{\infty} a_n x^n : a_n \in F \right\}, \quad m \in \mathbb{Z}$$

"Laurent series"



$$\frac{x}{x} \cdot \frac{x^{-3} + 2x^{-2} - x^{-1} - 1 + 2x + 3x^2 + \cdots}{x^{-1} + 1 + x + x^2 + x^3 + \cdots} = \frac{x^{-2} + 2x^{-1} - 1 - x + 2x^2 + 3x^3 + \cdots}{1 + x + x^2 + x^3 + x^4 + \cdots} = x^{-2} + x^{-1} - 3 + 3x^2 + \cdots$$

$$x^{-2} + 2x^{-1} - 1 - x + 2x^2 + 3x^3 + \cdots = (1 + x + x^2 + x^3 + x^4 + \cdots)(x^{-2} + x^{-1} - 3 + 3x^2 + a_3 x^3 + a_4 x^4 + \cdots)$$

$$= x^{-2} + 2x^{-1} - 1 - x + 2x^2 + \cdots$$

$$\frac{x^3}{x^3} \cdot \frac{x^{-1} + 1 + x + x^2 + x^3 + \cdots}{x^{-3} + 2x^{-2} - x^{-1} - 1 + 2x + 3x^2 + \cdots} = x^2 + b_3 x^3 + b_4 x^4 + b_5 x^5 + b_6 x^6 + \cdots$$

$$= \frac{x^2 + x^3 + x^4 + x^5 + x^6 + \cdots}{1 + 2x - x^2 - x^3 + 2x^4 + 3x^5 + \cdots} = x^2 + b_3 x^3 + b_4 x^4 + b_5 x^5 + \cdots$$

Every rational function in $F(x)$ expands as a Laurent series.

eg. $\frac{1}{x^2-x-1} = -\frac{1}{1+x-x^2} = -1 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + \cdots$ (with $a_1 = 1$, $a_2 = -2$, $a_3 = 3$)

First way to expand

Multiply both sides by $1+x-x^2$:

$$-1 = (1+x-x^2)(-1 + x - 2x^2 + 3x^3 - 5x^4 + 8x^5 + \cdots)$$

$$\frac{1}{x^2-x-1} = -1 + x - 2x^2 + 3x^3 - 5x^4 + 8x^5 - 13x^6 + 21x^7 - 34x^8 + \cdots$$

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + \cdots$$

$$\frac{1}{1-2x} = 1 + 2x + 4x^2 + 8x^3 + 16x^4 + \cdots$$

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + x^4 - x^5 + \cdots$$

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 + 5x^4 + 6x^5 + \cdots$$

Square both sides or take $\frac{d}{dx}$ of both sides

OR: $f(x) = \frac{1}{x^2-x-1}$

Taylor series $\sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n = f(0) + f'(0)x + \frac{f''(0)}{2}x^2 + \frac{f'''(0)}{6}x^3 + \cdots$

$= -1 + x - 2x^2 + 3x^3 - \cdots$

Second way to expand

$$f'(x) = \frac{(x^2-x-1)\cdot 0 - 1\cdot(2x-1)}{(x^2-x-1)^2} = \frac{1-2x}{(x^2-x-1)^2}$$

$f''(x) = \cdots$ $f'''(x) = \cdots$

Third way

$$\frac{1}{x^2-x-1} = -\frac{1}{1+x-x^2} = -\frac{1}{1-(x^2-x)} = -\left[1 + (x^2-x) + (x^2-x)^2 + (x^2-x)^3 + (x^2-x)^4 + \cdots\right]$$

$$= -\left[1 + x^2 - x + x^4 - 2x^3 + x^2 + x^6 - 3x^5 + 3x^4 - x^3 + x^8 - 4x^7 + 6x^6 - 4x^5 + x^4 + \cdots\right]$$

$$= -1 + x - 2x^2 + 3x^3 - 5x^4 + \cdots$$

Fourth way gives explicit coefficients

$$\frac{1}{x^2-x-1} = -\frac{1}{1+x-x^2} = -\frac{1}{(1-\alpha x)(1-\beta x)}$$

$$= \frac{A}{1-\alpha x} + \frac{B}{1-\beta x}$$ partial fraction decomposition

$$A(1-\beta x) + B(1-\alpha x) = -1$$

Evaluate at $\frac{1}{\alpha}$, $\frac{1}{\beta}$ to solve for A, B:

$$A\left(1-\frac{\beta}{\alpha}\right) = -1 \Rightarrow A(\alpha-\beta) = -\alpha \Rightarrow A = \frac{\alpha}{\sqrt{5}}$$

$$B\left(1-\frac{\alpha}{\beta}\right) = -1 \Rightarrow B(\beta-\alpha) = -\beta \Rightarrow B = -\frac{\beta}{\sqrt{5}}$$

$$\frac{1}{x^2-x-1} = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x}$$

$$= A\sum_{n=0}^{\infty}(\alpha x)^n + B\sum_{n=0}^{\infty}(\beta x)^n$$

$$= \sum_{n=0}^{\infty}(A\alpha^n + B\beta^n)x^n$$

The coefficient of x^n is $A\alpha^n + B\beta^n = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} = \frac{\left(\frac{-1-\sqrt{5}}{2}\right)^{n+1} - \left(\frac{-1+\sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}}$

α, β are the reciprocal roots of $1+x-x^2$

i.e. $\frac{1}{\alpha}, \frac{1}{\beta}$ are the roots

i.e. roots of $1+\frac{1}{x}-\frac{1}{x^2} = \frac{x^2+x-1}{x^2} = \frac{(x-\alpha)(x-\beta)}{x^2}$

i.e. α, β are the roots of $x^2+x-1 = (x-\alpha)(x-\beta)$

$$\alpha, \beta = \frac{-1 \pm \sqrt{1+4}}{2} = \frac{-1 \pm \sqrt{5}}{2}$$

$$\alpha = \frac{-1-\sqrt{5}}{2} = -\tau, \quad \tau = \frac{1+\sqrt{5}}{2} = 1.618\ldots$$ Golden ratio

$$\beta = \frac{-1+\sqrt{5}}{2} = \tau - 1 \approx 0.618$$

$$\alpha - \beta = \frac{-1-\sqrt{5}}{2} - \frac{-1+\sqrt{5}}{2} = -\sqrt{5}$$

$$\beta - \alpha = \sqrt{5}$$

Find the inverse of 5 and 3 mod 512!

Euclid's algorithm

512	5	
1	0	512
0	1	5
1	−102	2
−2	205	[1] ←
*	*	0

$1 = -2 \cdot 512 + 5 \cdot 205$

Inverse of 5 mod 512 is 205.

$(5 \cdot 205 = 1025 \equiv 1 \bmod 512)$

Another way to do this:

$\frac{1}{5} = \frac{1}{1+4} = 1 - 4 + 16 - 64 + 256 - 1024 + \cdots \equiv 205 \bmod 512.$

$273 - 68 = 205$

$0 \bmod 512$

$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$

$\frac{1}{1+x} = 1 - x + x^2 - x^3 + x^4 - \cdots$

512	3	
1	0	512
0	1	3
1	−170	2
−1	171	[1]
*	*	0

$1 = 171 \cdot 3 - 1 \cdot 512$

Inverse of 3 mod 512 is 171

$\frac{1}{3} = -\frac{1}{1-4} = -(1 + 4 + 64 + 256 + 1024 + \cdots) \equiv -(273 + 68) \equiv -341 \equiv 171$

Check: $7 \times 439 = 3073 \equiv 1 \bmod 512$

Inverse of 7 mod 512 is

$\frac{1}{7} = -\frac{1}{1-8} = -(1 + 8 + 64 + 512 + \cdots) \equiv -73 \equiv 439 \bmod 512$

0

$1 + 2 + 4 + 8 + 16 + 32 + \cdots = -1 = \frac{1}{1-2} = \frac{1}{-1}$

S

$S = 1 + 2 + 4 + 8 + 16 + \cdots = 1 + 2S \Rightarrow -S = 1 \Rightarrow S = -1.$

$2S = 2 + 4 + 8 + 16 + 32 + \cdots$

Eg. $F = \mathbb{F}_2 = \{0, 1\}$

In $F(x)$, $f(x) = \frac{x + x^4}{1 + x + x^3}$, $g(x) = \frac{1 + x^2 + x^3}{x + x^2}$;

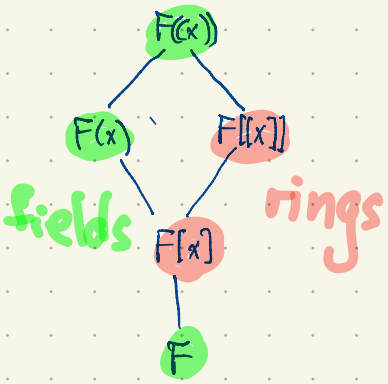
$$f(x)g(x) = \frac{(x+x^4)(1+x^2+x^3)}{(1+x+x^3)(x+x^2)} = \frac{(1+x^3)(1+x^2+x^3)}{(1+x+x^3)(1+x)}$$

$$f(x) + g(x) = \frac{(x+x^4)(x+x^2) + (1+x^2+x^3)(1+x+x^3)}{(1+x+x^3)(x+x^2)}$$

$$= \frac{1 + x^2 + x^3 + x^6}{1 + x^2 + x^3 + x^4}$$

$$= \frac{(1+x)(1+x+x^5)}{(1+x)(1+x+x^3)}$$

$$= \frac{1+x+x^5}{1+x+x^3}$$



Expand $f(x)g(x)$ as a power series:

$$\frac{1+x+x^5}{1+x+x^3} = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + \cdots = 1 + x^3 + x^4 + x^5 + \cdots$$

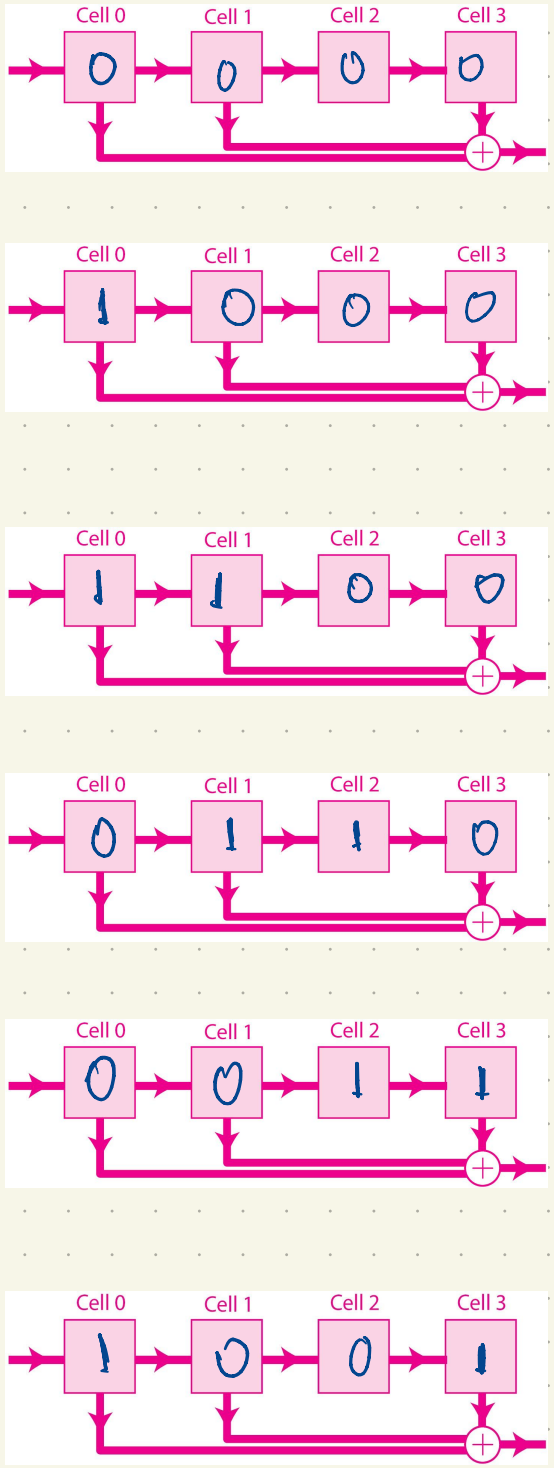
$$1 + x + x^5 = (1 + x + x^3)(1 + x^3 + x^4 + a_5 x^5 + \cdots)$$

Applications of algebra include
- cryptography — security, authentication, etc.
- error-correcting codes (coding theory)

Imagine a digital camera outputs a stream of bits (0's and 1's) as 110010…
If we replace $0 \to 000$, $1 \to 111$ then we are encoding the stream as 111111000000111000…
111101000000111000…

Represent our stream of bits $(a_0, a_1, a_2, a_3, \cdots)$, $a_i \in \mathbb{F}_2 = \{0, 1\}$ as a power series $f(x) = \sum_{n=0}^{\infty} a_n x^n = 1 + x + x^4 + \cdots$

One step in encoding is to transform $f(x)$ to a new series $\hat{f}(x) = g(x) f(x)$ where $g(x) \in F[x]$ or $g(x) \in F(x)$.



forward shift register

$$\hat{f}(x) = (1 + x + x^3)(1 + x + x^4 + \cdots)$$
$$= 1 + x^2 + x^3 + \cdots$$

To multiply two power series is the same thing as to convolve two sequences of numbers:

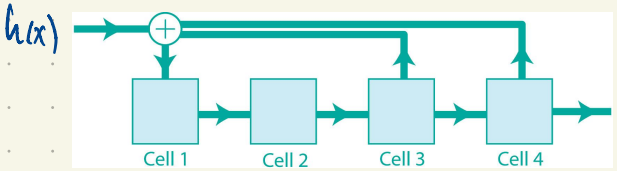
$$f(x)g(x) = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} a_n b_m x^{m+n} = \sum_{k=0}^{\infty}\left(\sum_{l=0}^{k} a_l b_{k-l}\right) x^k$$

add / multiply / convolve / solve — addition / multiplication / convolution / solution

$$f(x) = \sum_{n=0}^{\infty} a_n x^n \qquad (a_0, a_1, a_2, \cdots) * (b_0, b_1, b_2, \cdots) = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_0 b_2 + a_1 b_1 + a_2 b_0,\ \ldots)$$

$$g(x) = \sum_{m=0}^{\infty} b_m x^m \qquad \int f(t)g(x-t)\,dt = (f * g)(x)$$

(* : convolve)



$\hat{h}(x)$ backward shift register

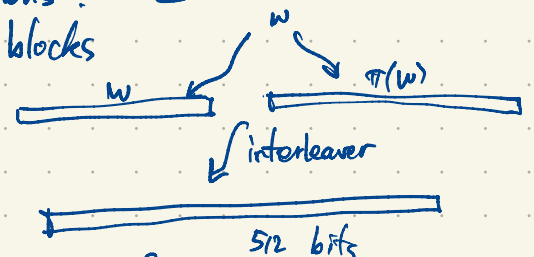
this is the inverse operation for the previous:

$$\hat{h}(x) = \frac{h(x)}{1 + x + x^3}$$

Typical codes used in practice: convolutional codes, turbo codes, ...

Stream of bits: 0011010000101010...

Split into blocks

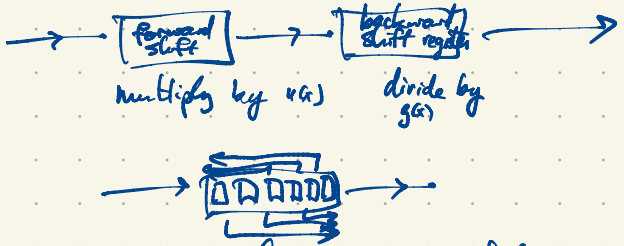


$\pi \in S_{256}$

multiply by $\frac{u(x)}{g(x)}$ (polynomials)

This is the encoded stream. (used for transmission)

Receiver multiplies by $\frac{g(x)}{m(x)}$



(F subfield of E).

If $E \supseteq F$ is an extension of fields then E is a vector space over F.

The degree of the extension, denoted $[E:F]$, is the dimension of this vector space.

eg. $[\mathbb{C}:\mathbb{R}] = 2$ with basis $\{1, i\}$ i.e. every $z \in \mathbb{C}$ is uniquely expressible as $z = a\cdot 1 + b\cdot i$, $a, b \in \mathbb{R}$.

eg. Let $\alpha \in \mathbb{C}$ be a root of $x^3 + x + 1 \in \mathbb{Q}[x]$ (irreducible) i.e. $\alpha^3 + \alpha + 1 = 0$. this gives an extension field

$E \supset \mathbb{Q}$, $E = \mathbb{Q}[\alpha] = \{\text{polynomials in } \alpha \text{ with rational coefficients}\} =$

$= \{a\cdot 1 + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$ has basis $\{1, \alpha, \alpha^2\}$

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

$\alpha^4 = -\alpha - \alpha^2$

$\alpha^5 = -\alpha^2 - \alpha^3 = -\alpha^2 + 1 + \alpha$

If $[E:F] = 1$ then $\{1\}$ is a basis for E over F. Every element of E has the form $a\cdot 1$, $a \in F$

$[E:\mathbb{Q}] = 3 = \deg(x^3 + x + 1)$

The only subfields of E are E and $\mathbb{Q}$. Proof: Suppose $F \subseteq E$ is a subfield. Then $E \supseteq F \supseteq \mathbb{Q}$ and $[E:\mathbb{Q}] = [E:F][F:\mathbb{Q}]$

$\mathbb{R} \supset \mathbb{Q}$ is an extension field but as a vector space over $\mathbb{Q}$, its dimension is infinite.

$[\mathbb{R} : \mathbb{Q}] = \infty$.

$\mathbb{R} \supseteq \mathbb{R}$ is one-dimensional : $[\mathbb{R} : \mathbb{R}] = 1$. $\{1\}$ is a basis.

Every real number is uniquely expressible as a real scalar multiple of 1.

a ⇓

$a = \underbrace{[a]}_{\text{real scalar}} \cdot 1$

Looking for a basis for $\mathbb{R}$ over $\mathbb{Q}$?

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19}, \sqrt{23}, \ldots$

$[\mathbb{C} : \mathbb{R}] = 2$ with basis $\{1, i\}$

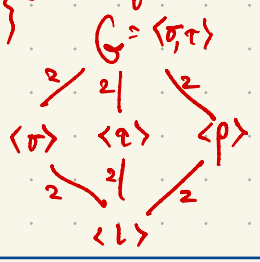
$[\mathbb{C} : \mathbb{C}] = 1$ with basis $\{1\}$.

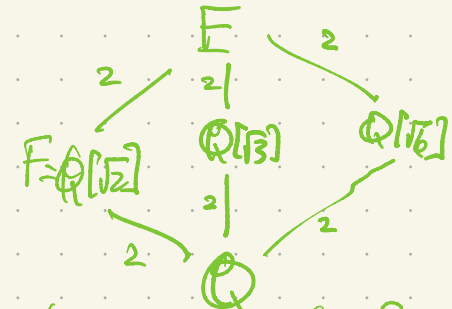
$[\mathbb{C} : \mathbb{Q}] = \infty$.

A Klein four-group

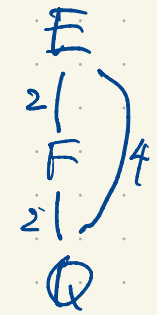
$G = \{1, \sigma, \tau, \rho\}$

	1	σ	τ	ρ
1	1	σ	τ	ρ
σ	σ	1	ρ	τ
τ	τ	ρ	1	σ
ρ	ρ	τ	σ	1





these are the only five subfields of this field E.



If $E \supseteq F \supseteq K$ is a tower of fields then

$$[E : K] = [E : F][F : K]$$

$$[\mathbb{C} : \mathbb{Q}] = [\mathbb{C} : \mathbb{R}][\mathbb{R} : \mathbb{Q}]$$

$\infty \quad 2 \quad \infty$

eg. $F = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \supset \mathbb{Q}$

$\{1, \sqrt{2}\}$ basis

$E = F[\sqrt{3}] = \{\alpha + \beta\sqrt{3} : \alpha, \beta \in F\}$ basis $\{1, \sqrt{3}\}$

$[E : \mathbb{Q}] = 4$

$[E : \mathbb{Q}] = [E : F][F : \mathbb{Q}]$

$4 \quad 2 \quad 2$

$\alpha = a + b\sqrt{2} \in F$

$\beta = c + d\sqrt{2} \in F$

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for E over $\mathbb{Q}$

Every element of E is uniquely expressible as

$$\alpha + \beta\sqrt{3} = (a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$a, b, c, d \in \mathbb{Q}$

$E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ = Span of $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

$E = \mathbb{Q}[\theta]$, $\theta = \sqrt{2}+\sqrt{3}$ = Span of $\{1, \theta, \theta^2, \theta^3\}$

$E = \{a + b\theta + c\theta^2 + d\theta^3 : a, b, c, d \in \mathbb{Q}\}$

$\theta^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\cdot\sqrt{2}\cdot\sqrt{3} = 5 + 2\sqrt{6}$

$\theta^2 - 5 = 2\sqrt{6}$

$(\theta^2 - 5)^2 = (2\sqrt{6})^2$

$\theta^4 - 10\theta^2 + 25 = 24$

$\theta^4 - 10\theta^2 + 1 = 0$

θ is a root of $x^4 - 10x^2 + 1$. Is this the minimal poly. of θ? i.e. is $x^4 - 10x^2 + 1$ irreducible over $\mathbb{Q}$?

If it has rational roots, then it has integer roots dividing 1 but ± 1 are not roots so no.

So $x^4 - 10x^2 + 1$ cannot have factorization as degree 1 times degree 3 in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$.

If $x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + b)$ $\quad b^2 = 1$, $b = \pm 1$

$a, b \in \mathbb{Z}$

then $x^4 - 10x^2 + 1 = (x^2 + ax + 1)(x^2 - ax + 1)$, $\quad a \in \mathbb{Z}$

$-10 = 2 - a^2 \Rightarrow a^2 = 12$, contradiction.

So $x^4 - 10x^2 + 1$ is the minimal poly. of $\theta = \sqrt{2}+\sqrt{3}$.

So θ is algebraic of degree 4:

$E = \mathbb{Q}[\theta] \supset \mathbb{Q}$ has degree 4. $\quad 1, \theta, \theta^2, \theta^3$ is a basis.

Shorter way to see that $\theta = \sqrt{2} + \sqrt{3}$ generates E.

Any thing of the form $\theta = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, $a, b, c, d \in \mathbb{Q}$ generates E as long as at least two of b, c, d are nonzero.

$c = d = 0$: $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$b = c = 0$: $a + d\sqrt{6} \in \mathbb{Q}[\sqrt{6}]$

$b = d = 0$: $a + c\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$

} In these cases θ generates either $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, or $\mathbb{Q}[\sqrt{6}]$.

Suppose $\theta \in \mathbb{C}$ is a root of some nonzero poly $m(x) \in \mathbb{Q}[x]$.
Then take the smallest degree such $m(x)$. Assuming $m(x)$ is monic, this is the minimal polynomial of θ (over $\mathbb{Q}$). It is irreducible in $\mathbb{Q}[x]$.
Conversely, if $m(x) \in \mathbb{Q}[x]$ is a monic irreducible poly. having θ as a root, then it is the minimal poly. of θ. (over $\mathbb{Q}$).
To find $m(x)$: look at $1, \theta, \theta^2, \theta^3, \dots$ until you find a power θ^n which is a linear combination of smaller powers $1, \theta, \theta^2, \dots, \theta^{n-1}$.
$\theta^n = a_0 \cdot 1 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1} \iff \theta$ is a root of $x^n - a_{n-1}x^{n-1} - \dots - a_1 x - a_0 \in \mathbb{Q}[x]$ (monic).