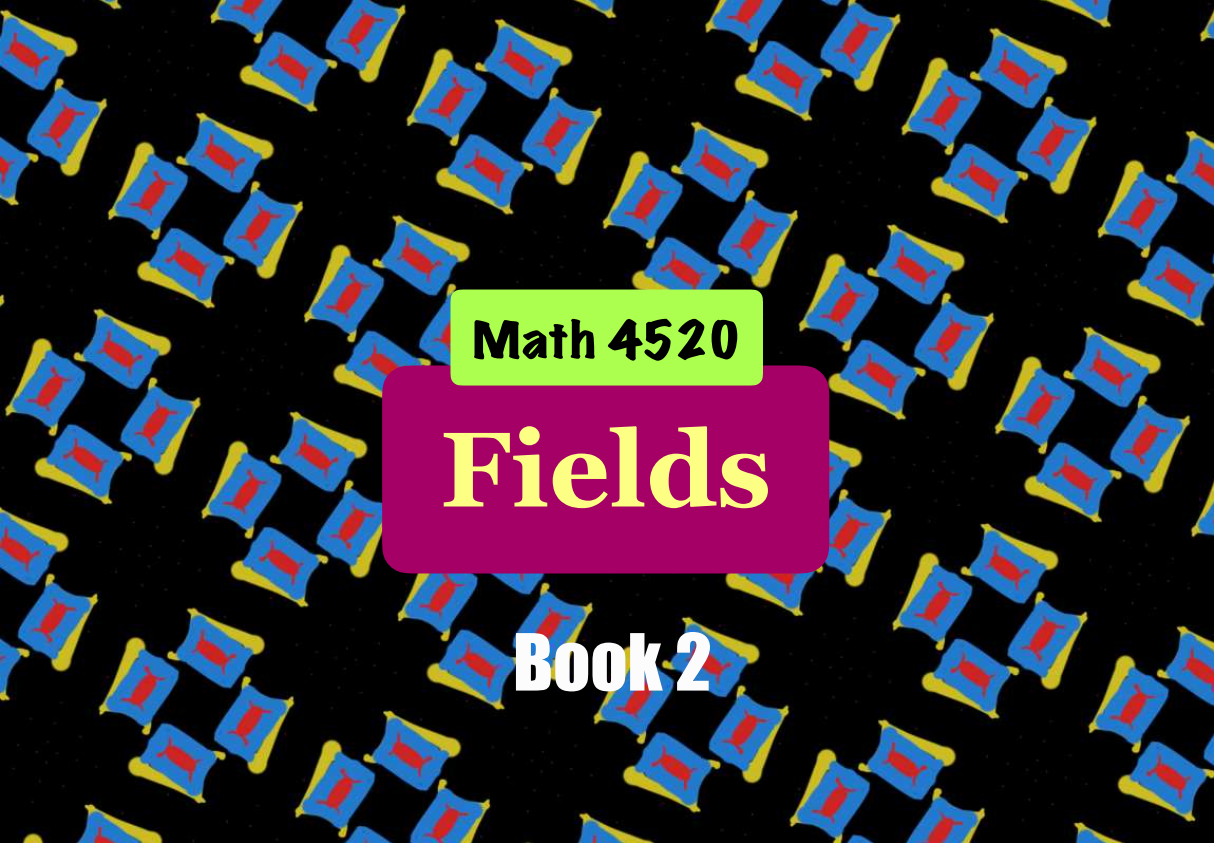




Math 4520

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: $x^2, x^2+1, x^2+x, x^2+x+1$
 $\underbrace{x^2}_{x \cdot x} \quad \underbrace{(x+1)^2}_{(x+1)(x+1)} \quad \underbrace{x(x+1)}_{x(x+1)} \quad \underbrace{x^2+x+1}_{\text{irreducible}}$
 $\underbrace{\hspace{10em}}_{\text{reducible}}$

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

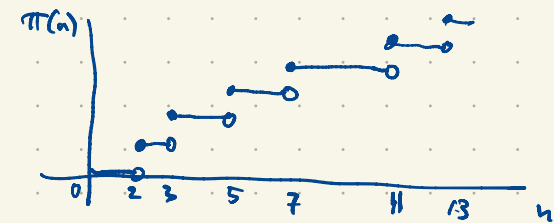
Given prime p , and integer $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

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



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

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

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 .

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\alpha^7 = 1$$

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

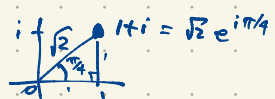
Multiplying elements of E is easier using the second description $E = \{0, 1, \alpha, \alpha^2, \dots, \alpha^6\}$.

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

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

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

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

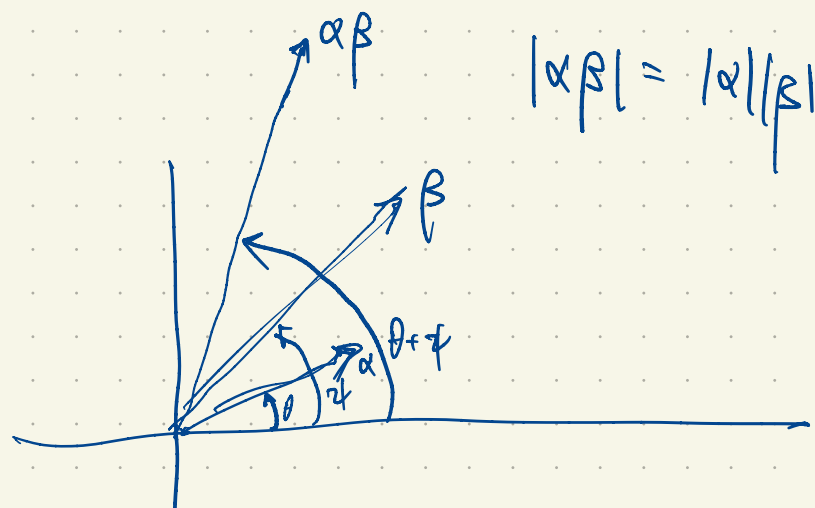
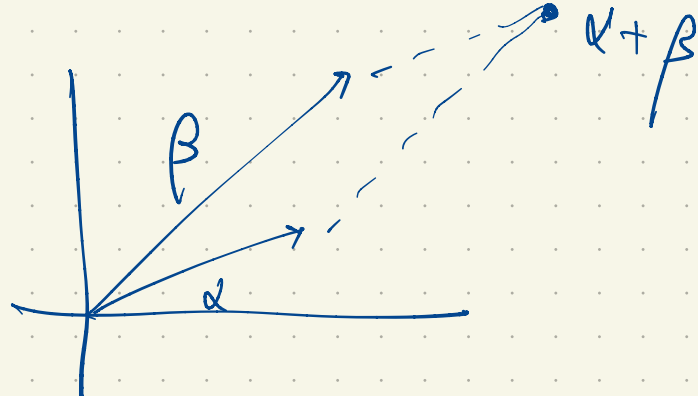


$$\sqrt{2} = 2^{1/2}$$

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

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

$$= e^{8\pi i} \cdot e^{5\pi i/4} = e^{5\pi i/4} = -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$$



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.

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