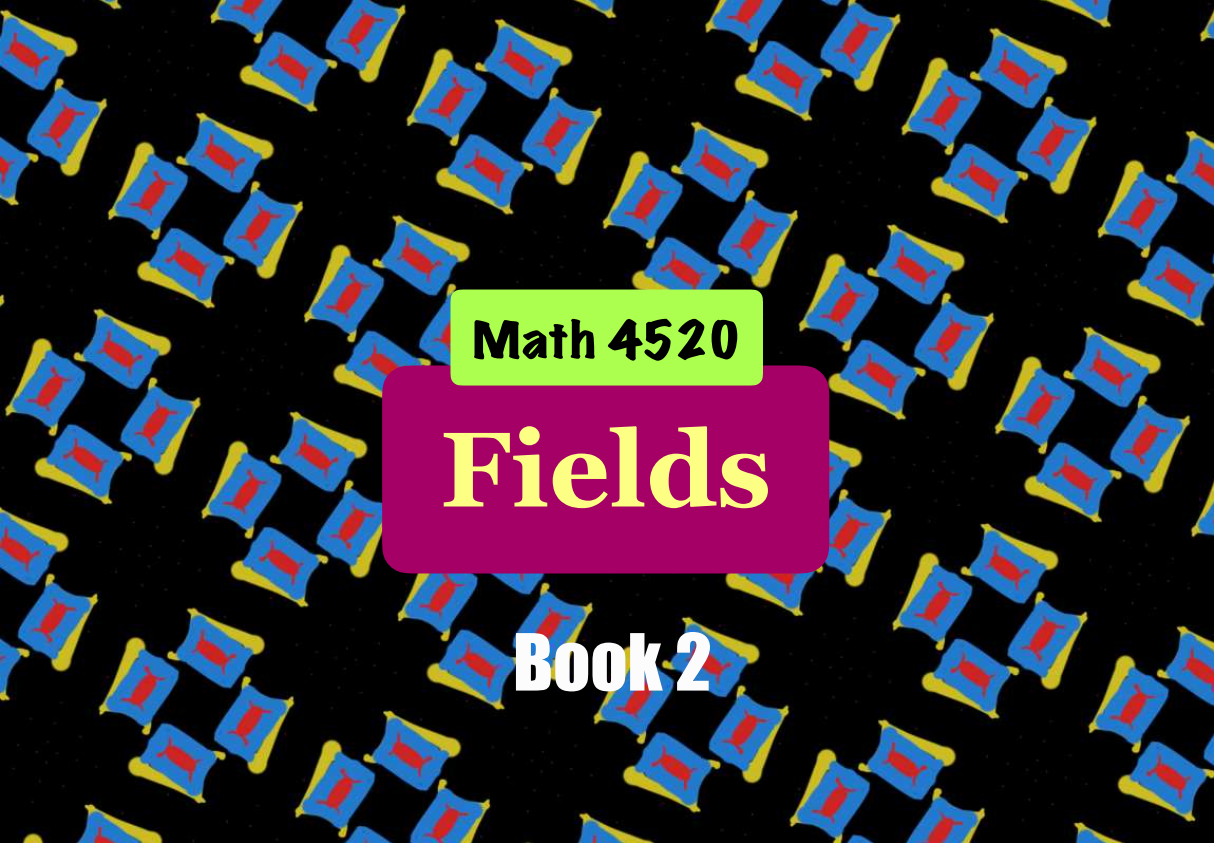




Math 4520

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: $x^2, x^2+1, x^2+x, x^2+x+1$
 $\begin{matrix} x \cdot x & (x+1)^2 & x(x+1) & \text{irreducible} \\ & = (x+1)(x+1) & & \\ & \text{reducible} & & \end{matrix}$

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

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

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

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

reducible

irreducible

$$\begin{matrix} x^4 + x^3 + x^2 + x + 1 \\ x^4 + x + 1 \\ x^4 + x^3 + 1 \end{matrix}$$

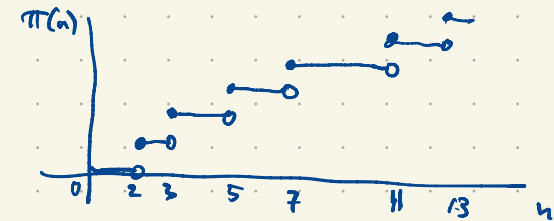
Given prime p , and integer $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

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.

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

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.
 $= \{0, 1, \alpha, \alpha + 1\}$