

Lecture 21 (Characteristic of a Field)

A Finite Field Example Consider the polynomial $p(x) = 1 + x + x^3$ in $\mathbb{F}_2[x]$. Because $p(1) = p(0) = 1$, $p(x)$ has no linear factor in $\mathbb{F}_2[x]$. Hence it is irreducible. (If a cubic is factorised into two factors one must be linear and the other a quadratic). Set $K = \langle p(x) \rangle$. Then we can construct an extension field E of \mathbb{F}_2 isomorphic to $\mathbb{F}_2[x]/K$ by relabelling $a + K$ as a for $a \in \mathbb{F}_2$ and $x + K$ as α :

$$\begin{aligned} 0 + K &\leftrightarrow 0, & 1 + K &\leftrightarrow 1, \\ x + K &\leftrightarrow \alpha, & 1 + x + K &\leftrightarrow 1 + \alpha, \\ x^2 + K &\leftrightarrow \alpha^2, & 1 + x^2 + K &\leftrightarrow 1 + \alpha^2, \\ x + x^2 + K &\leftrightarrow \alpha + \alpha^2, & 1 + x + x^2 + K &\leftrightarrow 1 + \alpha + \alpha^2. \end{aligned}$$

where $1 + \alpha + \alpha^3 = p(\alpha) = 0$. See E is a field with 8 distinct elements,

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

To multiply two arbitrary elements directly we just need to know α^3 and α^4 in terms of $1, \alpha, \alpha^2$: $\alpha^3 = 1 + \alpha$, and $\alpha^4 = \alpha + \alpha^2$.

Continuing multiplying by α and replacing α^3 by $1 + \alpha$ we can list all the powers of α :

$$\begin{aligned} \alpha^5 &= \alpha^2 + (1 + \alpha) = 1 + \alpha + \alpha^2 \\ \alpha^6 &= \alpha + \alpha^2 + (1 + \alpha) = 1 + \alpha^2 \\ \alpha^7 &= \alpha + (1 + \alpha) = 1 \end{aligned}$$

The non-zero elements E^\times of E form a cyclic group under multiplication of 7. Every element of E^\times is a power of α .

We can now find inverses to each non-zero element, using $\alpha^{-i} = \alpha^{7-i}$. We have $1^{-1} = 1$ and

$$\begin{aligned} \alpha^{-1} &= \alpha^6 = 1 + \alpha^2, & (1 + \alpha^2)^{-1} &= 1 + \alpha \\ \alpha^{-2} &= \alpha^5 = 1 + \alpha + \alpha^2, & (1 + \alpha + \alpha^2)^{-1} &= \alpha^2 \\ (1 + \alpha)^{-1} &= \alpha^{-3} = \alpha^4 = \alpha + \alpha^2 & (\alpha + \alpha^2)^{-1} &= 1 + \alpha \end{aligned}$$

For all x, y in a ring of commutative ring or field like E where $2 = 1 + 1 = 0$ $(x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$. Since also $(xy)^2 = x^2y^2$, squaring is a field homomorphism from E to E .

Hence from $1 + \alpha + \alpha^3 = 0$ we deduce $1 + \alpha^2 + (\alpha^2)^3 = 0$ and $1 + \alpha^4 + (\alpha^4)^3 = 0$. So $p(x)$ has roots α, α^2 and α^4 . So $p(x)$ factorised completely in E :

$$x^3 + x + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4).$$

Definition 20.1 (Characteristic of a Field) Suppose R is a ring with a unit element. If $n1 = 1 + 1 \cdots + 1 \neq 0$ for any $n = 1, 2, \dots$, we say R has characteristic 0. Otherwise $n1 = 1 + 1 \cdots + 1 = 0$ for some $n \geq 1$. In this case the smallest such n is called the characteristic of R .

Examples

- All of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0.
- The ring $\mathbb{Z}/m\mathbb{Z}$ has characteristic $m = 0, 1, 2, \dots$
- In particular a finite field with p elements $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{N}$ prime has characteristic p .

Proposition 20.2 The characteristic of an integral domain is either 0 or a prime number $p > 0$.

Proof In an integral domain $1 \neq 0$, so if $n1 = 0$, $n > 1$. If n is composite $n = rs$, for integers $n > r, s > 1$, then $(r1)(s1) = (rs)1 = 0$. An integral domain has no zero divisors. So in an integral domain, we deduce $r1 = 0$ or $s1 = 0$, contradicting the minimality of n . \square

Corollary The characteristic of a field is either 0 or a prime number p .

Examples (Field of Characteristic $p > 0$)

- If $p \equiv 3 \pmod{4}$, $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a field of characteristic p .
- For $m(x) \in \mathbb{F}_p[x]$ is irreducible, the field $F_p[x]/m(x)F_p[x]$ has characteristic p . If $\deg m(x) = d$ then $F_p[x]/m(x)F_p[x]$ is a finite field with p^d elements. Such a field is called a *Galois Field*.
- The rational function field $\mathbb{F}_p(x)$, (quotient field of $\mathbb{F}_p[x]$), has characteristic p and has infinitely many elements.