Intro to Algebra W2-2

fat

February 28, 2024

9.5 Polynomial rings over fields

Let F be a field. Recall that $F[x]$ is a ED, PID, UFD.

Proposition 15. Let $f(x) \in F[x]$. $F[x]/(f(x))$ is a field $\Leftrightarrow$ $(f(x))$ is a maximal ideal $\Leftrightarrow$ $f(x)$ is a irreducible polynomial in $F[x]$.

Proof.

Recall that in a PID (that is not a field), (a) is a maximal ideal $\Leftrightarrow$ a is an irreducible. $\square$

Construction of finite fields of p^n elements

Idea: Let p be a prime. Let F_p denote the field $\mathbb{Z}/p\mathbb{Z}$. Let $f(x)$ be an irreducible polynomial of degree n in $F_p[x]$. By Proposition 15, $F_p[x]/(f(x))$ is a field. We claim that the number of elements in $F_p[x]/(f(x))$ is p^n. By Theorem 3, $\forall a(x) \in F_p[x], \exists! q(x), r(x) \in F_p[x]$ s.t.

$$\begin{cases} a(x) = q(x)f(x) + r(x) \\ r(x) = 0 \text{ or } deg(x) < deg(f) \end{cases}$$

This implies that in any coset $a(x) + (f(x))$, there is a unique $r(x) = 0$ or $deg(r) < deg(f)$ (this $r(x)$ is obtained by the division algorithm in Theorem 3). Therefore $\{a_{n-1}x^{n-1} + \ldots + a_0 : a_j \in F_p\}$ forms a complete set of coset representatives of $(f(x))$ in $F_p(x) \Rightarrow |F_p[x]/(f(x))| = p^n$.

Summary: To construct a field of p^n elements, we simply find an irreducible polynomial of degree n in $F_p[x]$. Then $F_p[x]/(f(x))$ is a field of p^n elements.

Example 1. $p = 2, n = 2$. Let $f(x) = x^2 + x + 1$. Then $f(x)$ is an irreducible polynomial in $F_2[x]$ (0, 1 are not roots of $f(x)$, so $f(x)$ is irreducible in $F_2[x]$). The table of $F_2[x]/(x^2 + x + 1)$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Proposition 16. If $f(x) = f_1(x)^{e_1} \dots f_k(x)^{e_k}$ where $f_i(x)$ are distinct irreducible polynomials in $F[x]$ that are not associates of each other. Then

$$F[x]/(g(x)) \simeq F[x]/(f_1(x)^{e_1}) \times \dots \times F[x]/(f_k(x)^{e_k})$$

Proof.

Note that in a PID R, if $GCD(a,b) = d$, then $\exists x, y \in R$ s.t. $ax + by = d$ (Prop 6 of Section 8.2). In a UFD, this is not the case. For example, $\mathbb{Z}[x]$ is a UFD. Now $GCD(2,x) = 1$, but there do not exist $r(x), s(x) \in \mathbb{Z}[x]$ s.t. $2r(x) + xs(x) = 1$. Therefore if $i \neq j$, then $(f_i(x)^{e_i}) + (f_j(x)^{e_j}) = (1) = R[x]$. By the CRT,

$$F[x]/(g(x)) \simeq F[x]/(f_1(x)^{e_1}) \times \dots \times F[x]/(f_k(x)^{e_k})$$

□

Proposition 17. A polynomial of degree n in $F[x]$ has at most n roots in F (with multipiplicities taken into account).

Proof.

We'll prove by induction on the degree of the polynomial. If $f(x) = ax - b, a \neq 0$, has degree 1, then clearly $f(\alpha) = 0 \Leftrightarrow \alpha = a^{-1}b$. The statement holds for polynomial of degree 1. Suppose that the statement holds for polynomials of degree up to $n-1$. Let $f(x)$ be a polynomial of degree n in $F[x]$. If $f(x)$ has no roots in F, we are done. If $f(x)$ has a root $\alpha \in F$, then $f(x) = (x - \alpha)g(x)$. Now if β is a root of $f(x)$ in $F[x]$, then

$$(\beta - \alpha)g(\beta) = 0$$

$$\Rightarrow \beta - \alpha = 0 \text{ or } g(\beta) = 0$$

$$\Rightarrow \beta = \alpha \text{ or } \beta \text{ is a root of } g(x)$$

By the induction hypothesis, $g(x)$ has at most $n-1$ roots in $F \Rightarrow f(x)$ has at most n roots in F. □

Proposition 18. Any finite subgroup of $F^\times$ is cyclic (In particular, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic).

Proof.

Let $G < F^{\times}$ be a finite subgroup. By the FTFGAG, we have

$$G \simeq (^{\mathbb{Z}}/_{n_1\mathbb{Z}}) \times \ldots \times (^{\mathbb{Z}}/_{n_k\mathbb{Z}})$$

for some positive integers n_j satisfying $n_k | n_{k-1} | \ldots | n_2 | n_1$. Then we have $a^{n_1} = 1 \ \forall a \in G \Rightarrow$ the polynomial $x^{n_1} - 1$ has at least $|G| = n_1 \ldots n_k$ roots in F. However, by Prop. 17, $x^{n_1} - 1$ has at most n_1 roots in $F \Rightarrow k = 1$ and $G \simeq \mathbb{Z}/n_1\mathbb{Z}$ is cyclic. $\square$