Abstract Algebra
: Lecture 16

Leo

2024.11.21

Theorem 1. *If D is UFD, then $D[x]$ is also UFD.*

证明. Finite factor chain condition is trivial. We want to prove if $f(x) = p_1(x) \dots p_s(x) = q_1(x) \dots q_t(x)$ then $s = t$ and $p_i(x) = q_j(x)$ for some i, j. This is equivalent to if $f(x)$ is irreducible, then $f(x)$ is prime.
Let $f(x) \in D[x]$ be irreducible. Assume $f|gh$. If $degf = 0$, we are done. Suppose $degf = n > 0$. Then $fq = gh$ for some $q \in D[x]$. Let K be fraction foeld of D. Then $f(x)$ is irreducible in $K[x]$, and so f is prime. Thus $f|g$ or $f|h$. Say $f|g$ i.e. $g(x) = f(x)d(x)$ in $K[x]$. Let r be the product of the denominators of the coefficients of $d(x)$. Then $rg(x) = f(x)(rd(x))$ in $D[x]$. Let $a = c(rg(x))$, $b = c(f(x)rd(x)) = c(rd(x))$. Then $ag_1(x) = bf(x)d_1(x)$, where g_1, f, d_1 are primitive. Then fd_1 also primitive by Gauss Lemma. So $a = bu$ where $u \in U(D)$ and $ug_1 = fd_1$, and so $f|g_1$, i.e. f is a prime element in $D[x]$. □

Now we begin with Field Theory.

Definition 2. *Let F be a field. If $F < E$ then F is a subfield of E, E is a extension of F.*

Definition 3. *Let $F < E$, let $S \subseteq E$, and let $F(S)$ be the intersection of all subfields of E containing S. $F(S)$ is called the field generated by S over F. In particular, if $S = \{a\}$ then $F(S) = F(a)$.*

Definition 4. *α is called algebraic element over F if $f(\alpha) = 0$ for some polonomial $f(x) \in F[x]$. Otherwise α is called transcendental element over F.*

Proposition 5. *Let $F < E$ and $\alpha \in E \setminus F$.*
(1). If α is transcendental, then $F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} | f, g \in F[x], g \neq 0\}$.
(2). If α is algebraic, then $F(\alpha) \simeq F[x]/(m(x))$, where $m(\alpha) = 0$ and $m|f$ if $f(\alpha) = 0$.

证明. Let $\sigma : F[x] \to F(\alpha)$ be the evaluation homomorphism. Let I be the kernel of σ. Then $F[x]/I \simeq F(\alpha)$. $I = \{f \in F[x] | f(\alpha) = 0\}$.
If α is transcendental, then $I = \{0\}$ and $F(\alpha) \simeq F[x]$.
If α is algebraic, then $I = (m(x))$, where $m(x)$ is the minimal polynomial of α over F. □

Example 6. *Find $\mathbb{F}_{p^2} > \mathbb{F}_p$, we need to find $x^2 - r$ and $x^2 - r$ irre. with $r \in \mathbb{F}_p$, then $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[x]/(x^2 - r)$.*

Theorem 7. *For any $n \in \mathbb{Z}^+$, there exist irreducible polynommial of deg n in $\mathbb{F}_p[x]$.*

证明. Just consider $n = 2$ There are exactly p^2 poly. with form $a + bx + x^2$. Among them, reducible ones are either $(a_0 + x)(a_0 + x)$ or $(a_0 + x)(a_1 + x)$, where $a_0 \neq a_1$. In total $p + \frac{1}{2}p(p-1) = \frac{1}{2}p(+1) < p^2$. $\square$

Exercise 8. $\mathbb{F}_3[x]/(x^2 + 1) \simeq \mathbb{F}_3[x]/(x^2 + x + 2)$