Abstract Algebra
: Lecture 17

Leo

2024.11.21

{b证}

Exercise 1. *Let F be a field, and $f(x) \in F[x]$, irreducible. Then there exists an extention E of F s.t. $f(x)$ has a root in E*

证明. Let $E = F[x]/(f(x))$. Since F is a field, $F[x]$ is a PID. $f(x)$ is irriducible shows $(f(x))$ is a maximal ideal hence E is a field. So $\bar{x}$ is a root of $f(x)$ in E since $f(\bar{x}) = \overline{f(x)} = 0$. □

Definition 2. *F is called a algebraic closed field if any polynomial $f(x) \in F[x]$ is reducible unless $deg f = 1$.*

Definition 3. *Let E/F be a field extension. Then E can be view as a vector space over F. If $\dim_F E = n$ is finite, then E is called a finite extension of F of degree n.*

Lemma 4. *If K/E is of degree m, E/F is of degree n, then K/F is of degree mn.*

P109

Construction by ruler(straightedge) and compasses.

Given a unit 1. $\in \mathbb{R}$

$\sqrt{a_n}$ alge over F_n. $f(\sqrt{a_n}) = 0$. $f \in F_{n+1}[x]$

(1). We can construct all integers.

(2). We can construct all rational numbers. 在R上最小多项式 $m_{\sqrt{a_n}, F_n}$ deg=1 或2

(3). We can construct all roots of quadratic polynomials. Q的扩域上 $x^2 - a_n$ 或 $x - a_n$

Now Let $F_0 = \mathbb{Q}$, $F_{n+1} = F_n(\sqrt{a_n})$ where a_n is a square-free integer. Then $[F_{n+1} : F_n]$ equal to 1 or 2. i.e. if α is constructible, then F_{n+1} is a finite extension of F_0 of degree of 2^k where $k \in \mathbb{Z}_{\geqslant 0}$.

先从 $x^2 - a_n$ 到 $x - a_n$

扩成整数 所以有R

Let F be a finite field.

obv

(1). Then $|F| = p^d$ where p is a prime number and $d \in \mathbb{Z}_{\geqslant 1}$.

(2). $(F, +) \simeq Z_p^d$. 加法群

(3). $(F^\times, *) \simeq Z_{p^d - 1}$. 看成乘法群

证明. (of (3)): Let m be the exponent of $F^\times$, m is the least common multiple of the order of elements of $F^\times$. Then each element t of $F^\times$ has order dividing m. So t is a root of $x^m - 1$. Let $a \in F^\times$ with $|a| = m$. Then $m = |a| \mid |F^\times|$ by Lagrange's theorem. So $m \leqslant p^d - 1$. ① On the other hand, $x^m - 1$ has at most m roots in F. So $m \geqslant p^d - 1$. ② So $m = p^d - 1$. And $F^\times \simeq Z_{p^d - 1}$. □

$F = \{x_1, x_2, \ldots\}$

$m = \gcd(o(x_1), o(x_2), \ldots)$

$\therefore o(t) \mid m$, $t^m = 1$

obv.. ②

①是什么? $|a| \times m = |F^\times| = p^d$? 不对

加法乘法还能用吗?

Consider the group action of multiple group on addition group, we can get a semidirect product of two groups such as $Z_p^d : Z_{p^d-1}$, denoted by $\mathrm{AGL}_1(p^d)$.
Let F be a finite field of order p^d, i.e. $\mathbb{F}_{p^d}$ or denoted by $\mathrm{GF}(p^d)$.

Theorem 5. *$\phi : F \to F$ s.t. $x \mapsto x^p$ is an automorphism of F.*

证明. Check: $(xy)^\phi = x^p y^p = x^\phi y^\phi$, $(x+y)^\phi = x^\phi + y^\phi$. This is called Frobenius automorphism. $\square$

Theorem 6. *Let F be a field of charateristic 0, then a finite extension of F is a simple extension.*

证明. Let $E = F(\alpha, \beta)$, Let $f(x), g(x)$ be irreducible polynomials in $F[x]$ s.t. $f(\alpha) = 0, g(\beta) = 0$. Let $\gamma = \alpha + c\beta$ where $c \in F$. We need to determine c s.t. $F(\alpha, \beta) = F(\gamma)$.
Let $h(x) = f(\gamma - cx) \in F(\gamma)[x]$, then $h(\beta) = f(\alpha) = 0$. So β is root of $h(x)$ and $g(x)$. If β is the only common root of $h(x)$ and $g(x)$, then $x - \beta = \gcd(g(x), h(x)) = s(x)g(x) + t(x)h(x) \in F(\gamma)[x]$.
So $\beta \in F(\gamma)$, and $\alpha = \gamma - c\beta \in F(\gamma)$. So $F(\alpha, \beta) = F(\gamma)$.
We will finish the proof next time. $\square$

gcd可以用这样求!