Rings II

Tuesday, August 6, 2024

## Field extensions

$F \subseteq E$

$[E:F]$ = dimension of $E$ as an $F$-vector space

Ex: $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$

$\mathbb{Q}(\sqrt[3]{2})$ spanned by $1, \sqrt[3]{2}, \sqrt[3]{4}$

$$[L:k][k:F] = [L:F]$$

---

## Finite fields

For each prime power $p^k$, there is a unique field of order $p^k$, up to isomorphism

$$[\mathbb{F}_{p^k} : \mathbb{F}_p] = k$$

$$\mathbb{F}_{p^j} \subseteq \mathbb{F}_{p^k} \iff j \mid k$$

In $\mathbb{F}_{p^k}$, every element satisfies $x^{p^k} = x$

$$x^{p^k} - x = \prod_{\alpha \in \mathbb{F}_{p^k}} (x - \alpha)$$

$\mathbb{F}_{p^k}$ is the "splitting field" $x^{p^k} - x$

$x \mapsto x^{p^k}$ is an automorphism of each finite field of order $p^j$, and $\mathbb{F}_{p^k}$ is its fixed field.

$x \mapsto x^p$ is an automorphism $\mathbb{F}_{p^j}$.

$$(xy)^p = x^p y^p \qquad (x+y)^p = x^p + y^p$$

---

$F$ is a field of characteristic $p$, and $\underbrace{1+1+\dots+1}_{p} = 0$

$\alpha$ is a root of $f(x) = x^p - x + 3$ in an extension of $F$, then $f(x)$ has $p$ distinct roots in $F(\alpha)$.

Solution: $f(x+1) = (x+1)^p - (x+1) + 3 = x^p + 1 - x - 1 + 3$
$= x^p - x + 3 = f(x)$

$$\underbrace{f(\alpha)=0, \quad f(\alpha+1)=0, \quad \dots, \quad f(\alpha+p-1)=0,}_{p \text{ distinct roots in } F(\alpha).}$$

---

Number Fields: Finite extension of $\mathbb{Q}$

- Quadratic Number Fields: $\mathbb{Q}(\sqrt{m})$, $m$ squarefree
  $(\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3}))$
  $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$
- Cyclotomic Fields: $\mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$
  $\zeta_n^n = 1$
  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) =$ number of integers $1 \le k \le n$ that have no common factors with $n$.
  $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$
  $\mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$
  $\zeta_n \mapsto \zeta_n^k$ for $k$ coprime to $n$
  is a field automorphism

---

Show that $\mathbb{Q}(\sqrt{p}) \not\cong \mathbb{Q}(\sqrt{q})$

Show that $\mathbb{Q}(\sqrt{p})$ has a squareroot of $p$ but $\mathbb{Q}(\sqrt{q})$ does not.

$\sqrt{p}^2 = p$

Suppose $(a + b\sqrt{q})^2 = p$

$$a^2 + b^2 q + \underbrace{2ab\sqrt{q}}_{=0} = p$$

$=0 \Rightarrow a = 0$ or $b = 0$

$b^2 q = p$ $\qquad$ $a^2 = p$

either case is contradictory.

---

$\theta \in \mathbb{R}$, $F_\theta = \mathbb{Q}(\sin\theta)$, $E_\theta = \mathbb{Q}(\sin\frac{\theta}{3})$

Show $F_\theta \subseteq E_\theta$ and determine possibilities

Show $F_\theta \subseteq E_\theta$ and determine possibilities for $[E_\theta : F_\theta]$.

---

$$e^{3i\theta} = (e^{i\theta})^3$$

$$\cos(3\theta) + i\sin(3\theta) = (\cos\theta + i\sin\theta)^3$$

$$= [\text{real part}] + i(3\cos^2\theta\sin\theta - \sin^3\theta)$$

$$\sin(3\theta) = 3\cos^2\theta\sin\theta - \sin^3\theta$$

$$= 3(1-\sin^2\theta)\sin\theta - \sin^3\theta$$

$$= 3\sin\theta - 4\sin^3\theta$$

$$3\sin\frac{\theta}{3} - 4\sin^3\frac{\theta}{3} = \sin\theta$$

$E_\theta$

$\sin\theta \in E_\theta$

$F_\theta \subseteq E_\theta$

If $\theta = 0$, and $F = \mathbb{Q}$, then

$$[\mathbb{Q}(\sin 0) : \mathbb{Q}(\sin 0)] = [\mathbb{Q}:\mathbb{Q}] = 1$$

If $\theta = \pi$ and $F = \mathbb{Q}$, then

$$[\mathbb{Q}(\sin\tfrac{\pi}{3}) : \mathbb{Q}(\sin\pi)] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$$

Pick $\theta = \frac{\pi}{6}$, then

$$3\sin\frac{\theta}{3} - 4\sin^3\frac{\theta}{3} - \frac{1}{2} = 0$$

$\sin\frac{\theta}{3}$ satisfies $3x - 4x^3 - \frac{1}{2} = 0$

$$x^3 - \frac{3}{4}x + \frac{1}{8} = 0$$

Show irred by RRT. $\rightsquigarrow$ degree 3.

$$[E_\theta : F_\theta] = [F_\theta(\sin\tfrac{\theta}{3}) : F_\theta] = \deg(\text{minpoly}(\sin\tfrac{\theta}{3}))$$

---

Show $\mathbb{Q}(t_1, \dots, t_n)$ = field of rational functions is isomorphic to a subfield of $\mathbb{R}$

e.g., $\dfrac{(t_1 + 2t_2)\, t_3^3}{t_4}$

$$\mathbb{Q}(t_1, \dots, t_n) \cong F \subseteq \mathbb{R}$$

$t_i \longmapsto$ some real numbers that are algebraically independent

Pick $t_1 \in \mathbb{R} \setminus \overline{\mathbb{Q}}$ (since $\mathbb{R}$ is uncountable but $\overline{\mathbb{Q}}$ is countable)

Pick $t_2 \in \mathbb{R} \setminus \overline{\mathbb{Q}(t_1)}$ and so on...

---

Pick $t_2 \in \mathbb{K} \setminus \mathbb{Q}(t_1)$ and so on...

---

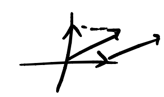
$G$ = group of invertible 2x2 matrices with entries in $\mathbb{F}_{p^n}$.

1) Show $|G| = (p^{2n}-1)(p^{2n}-p^n)$

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \text{ invertible} \iff \underbrace{\begin{bmatrix} a \\ b \end{bmatrix}}_{p^{2n}-1} \text{ and } \underbrace{\begin{bmatrix} c \\ d \end{bmatrix}}_{p^{2n}-p^n} \text{ linearly independent}$$

2) Show $p$-Sylow of $G$ is isomorphic to $(\mathbb{F}_{p^n}, +)$

(Show $G$ has a subgroup isomorphic to $(\mathbb{F}_{p^n}, +)$)



$$(\mathbb{F}_{p^n}, +) \cong \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \quad \text{since} \quad \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

---

Fact: $\mathbb{F}_{p^k}^\times$ is cyclic (more generally, any finite subgroup of $F^\times$ is cyclic)

(since $x^d - 1 = 0$ has at most $d$ roots)

---

How many elements of $\mathbb{F}_p$ have squareroots? Cuberoots?

$0$ has a squareroot and cuberoot.

$$\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \qquad |im| = \frac{|G|}{|ker|} = \frac{p-1}{|ker|}$$

$x \mapsto x^2$ $\quad x \mapsto 2x \to$ kernel $= \{0, \frac{p-1}{2}\}$

$x \mapsto x^3$ $\quad x \mapsto 3x \to$ kernel $= \begin{cases} \{0, \frac{p-1}{3}, \frac{2(p-1)}{3}\} & p \equiv 1 \pmod 3 \\ \{0\} & p \not\equiv 1 \pmod 3 \end{cases}$

---

last digit of $17^{(17^{17})}$, want $17^{(17^{17})} \bmod 10$

If $(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod n$ $\quad a^4 \equiv 1 \pmod n$

(Alternatively, $17^1 \equiv 7 \pmod{10}$ $\quad 17^2 \equiv 7^2 \equiv 9 \pmod{10}$
$17^3 \equiv 7^3 \equiv 7 \cdot 9 \equiv 3 \pmod{10}$, $17^4 \equiv 7^4 \equiv 9^2 \equiv 1 \pmod{10}$)

$17^{17} \equiv 1^{17} \equiv 1 \pmod 4$

$17^{17^{17}} \equiv 17^1 \equiv 17 \equiv 7 \pmod{10}$

---

| Positive Definite | Positive Semidefinite |
|---|---|
| (M is a symmetric real matrix) | |
| - M h positive eigenvalues | - M has nonnegative eigenvalues |
| - $x^T M x$ for $x \neq 0$ | - $x^T M x \geq 0$ |
| - $\langle x, Mx \rangle > 0$ for $x \neq 0$ | - $\langle x, Mx \rangle \geq 0$ |
| - $M = A^T A$ for invertible | - $M = A^T A$ for $A$ any matrix |