Field extensions $F \subseteq E$, $[E:F] = \dim$ of E
E/F as an F-vector space

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a,b,c \in \mathbb{Q}\}$$

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \qquad F \subseteq K \subseteq L$$

$$[L:F] = [L:K][K:F]$$

Finite fields $\quad \mathbb{F}_p$ p prime, $\quad \mathbb{F}_{p^k}$ with p^k elements

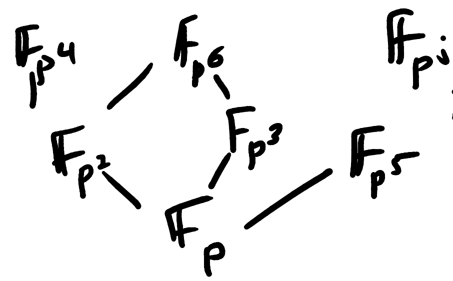
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

<u>unique</u> finite field (up to isomorphism) of each prime power p^k

$\mathbb{F}_p(\sqrt{a}) \quad \mathbb{F}_p \times \mathbb{F}_p$
$(1,0)\cdot(0,1)$

$$\mathbb{F}_7(\sqrt{3}) \cong \mathbb{F}_7(\sqrt{6})$$

$$\mathbb{F}_7(\sqrt{6}) = \mathbb{F}_7(3\sqrt{3})$$



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

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

$$\mathbb{F}_{p^k}^\times = \{a \in \mathbb{F}_{p^k} \mid a \neq 0\} \text{ is a group}$$

$\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) \cong \mathbb{Z}/k\mathbb{Z}$ generated by $x \mapsto x^p$.

$$a^{(p^k-1)} = 1, \quad a^{(p^k)} = a$$

Every element of $\mathbb{F}_{p^k}$ is a root of $x^{p^k} - x$

$$x^{p^k} - x = \prod_{a \in \mathbb{F}_{p^k}} (x - a) \quad \text{in } \mathbb{F}_{p^k}[x]$$

$\mathbb{F}_p[x]$

$$\left.\begin{array}{l} x \mapsto x^{p^k} \\ x \mapsto x^p \end{array}\right\} \text{Field automorphism}$$

$\mathbb{F}_{p^k}$ is the fixed set of $x \mapsto x^{p^k}$

$$(xy)^p = x^p y^p$$

$$(x+y)^p = x^p + y^p$$

$\mathbb{F}_{p^k}$ is the fixed field of $x \mapsto x^{p^k}$ $\quad (xy)^p = x^p y^p$

$\mathbb{F}_p((t))$ $\quad (x+y)^p = x^p + y^p$

$\mathbb{F}_p \subseteq F$ $\underbrace{\text{char } p}_{\underbrace{1+\cdots+1}_{p}=0} > 0$, α root of $x^p - x + 3 = f(x)$

show $f(x)$ has p distinct roots in $F(\alpha)$.

$f'(x) = -1$

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

α root

$\Rightarrow \alpha + 1$ root

$\vdots$

$\alpha + (p-1)$ roots

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

$\mathbb{Q}(\sqrt{m})$, m squarefree, degree 2 over $\mathbb{Q}$

$\mathbb{Q}(\zeta_n)$, $n \geq 1$, $\zeta_n = e^{2\pi i/n}$ $\quad$ minimal poly $\Phi_n = \dfrac{x^n - 1}{\prod_{\substack{d \mid n \\ d<n}} \Phi_d}$

$\zeta_n^n = 1 \quad x^n - 1 = 0$

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \#\{1 \leq k \leq n \mid \gcd(k, n) = 1\}$$

$\varphi(n) = p_1^{a_1 - 1}(p_1 - 1) \cdots p_j^{a_j - 1}(p_j - 1)$

$\varphi(n)$ automorphisms

$\zeta_n \mapsto \zeta_n^k$

6.12.14: $\underbrace{\mathbb{Q}(\sqrt{p})}_{\text{has } \sqrt{p}} \not\subseteq \underbrace{\mathbb{Q}(\sqrt{q})}_{\text{does not}}$

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

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

$a = 0$ or $b = 0 \rightsquigarrow$ contradiction

$E = \mathbb{Q}(\sin\theta)$, $E_3 = \mathbb{Q}(\sin\frac{\theta}{3})$

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

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

$$\left(\cos\frac{\theta}{3} + i\sin\frac{\theta}{3}\right)^3 = \left(e^{i\theta/3}\right)^3 = e^{i\theta} = \cos\theta + i\sin\theta$$

$$(\text{———}) + i\underbrace{\left(3\cos^2\frac{\theta}{3}\sin\frac{\theta}{3} - \sin^3\frac{\theta}{3}\right)}_{\sin\theta}$$

$$\sin\theta = 3\left(1 - \sin^2\frac{\theta}{3}\right)\sin\frac{\theta}{3} - \sin^3\frac{\theta}{3}$$

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

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

deg ≤ 3

$\theta = 0$, $E_\theta = \mathbb{Q}$, $F_\theta = \mathbb{Q}$ 1

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

$\theta = \frac{\pi}{6} \rightsquigarrow$ deg 3

Show $\underbrace{\mathbb{Q}(t_1, \ldots, t_n)} \hookrightarrow \mathbb{R}$

$$\frac{t_2 t_3 - t_4^2}{t_5 + 3}$$

Pick images for $t_1, \ldots, t_n$

$\overline{\mathbb{Q}(t_1, \ldots, t_{n-1})}$ countable

so $\exists\, t_n \in \mathbb{R} \setminus \overline{\mathbb{Q}(t_1, \ldots, t_{n-1})}$

Any finite subgroup of $\underbrace{\text{a field}}$ is cyclic.

Any finite subgroup of $\underbrace{\text{a field}}_{F^\times}$ is cyclic.

($x^d - 1 = 0$ has $\le d$ solutions)

(then some group theory)

$\mathbb{F}_p^\times$ cyclic of order $p-1$

$\mathbb{F}_{p^k}^\times$ cyclic of order $p^k - 1$

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

image of the squaring/cubing map

$$\mathbb{F}_p^\times \to \mathbb{F}_p^\times$$
$$x \mapsto x^2$$

how many $x^2 = 1$

how many $x^3 = 1$

$$\frac{|\mathbb{F}_p^\times|}{|\ker|} = |\mathrm{im}|$$

$$\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

$x^2 = 1 \longleftrightarrow 2y \equiv 0 \pmod{p-1} \to \{0, \frac{p-1}{2}\}$

$x^3 = 1 \longleftrightarrow 3y \equiv 0 \pmod{p-1} \longleftrightarrow \{0\}$ $p \not\equiv 1 \pmod 3$

$\to \{0, \frac{p-1}{3}, 2\frac{p-1}{3}\}$ if $p \equiv 1 \pmod 3$

M symmetric$/\mathbb{R}$

pos def	pos semidef
pos eigenvalues	nonneg eigenvalues
$\forall x$ $x^T M x > 0$	$\forall x$ $x^T M x \ge 0$
$\forall x$ $\langle x, Mx \rangle > 0$	$\forall x$ $\langle x, Mx \rangle \ge 0$
$M = A^T A$, A invertible	$M = A^T A$, A any matrix