$F \subseteq E$ field

$[E:F]$ = dimension of E as a vector space over F

E.g. $\mathbb{Q}(\sqrt[3]{2})$ = generated over $\mathbb{Q}$ by $1, \sqrt[3]{2}, \sqrt[3]{2}$

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

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

Finite fields

p a prime $\quad \mathbb{F}_p$ = integers mod p

For each $k \geq 1$, $\mathbb{F}_{p^k}$ is a field extension of $\mathbb{F}_p$,

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

$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n.$

Every element of $\mathbb{F}_{p^k}$ satisfies $x^{p^k} = x$

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

$\mathbb{F}_{p^k}$ is the splitting field of $x^{p^k} - x$ over $\mathbb{F}_p$.

The map $x \mapsto x^{p^k}$ is a field automorphism, (Frobenius automorphism)

$(x+y)^p \equiv x^p + y^p \pmod p$. fixes $\mathbb{F}_{p^k}$ pointwise

---

F is a field of char $p > 0$, ($p \neq 3$, ← not necessary) α is a root of $x^p - x + 3$ in an extension of F.

Show $x^p - x + 3$ has p distinct roots in $F(\alpha)$.

$(\alpha+1)^p - (\alpha+1) + 3 = \alpha^p + 1^p - (\alpha+1) + 3 = \alpha^p - \alpha + 3 = 0$

$(\alpha+2)^p - (\alpha+2) + 3 = \alpha^p + 2^p - (\alpha+2) + 3 = \alpha^p - \alpha + 3 = 0$

$(2^p \equiv 2 \pmod p)$

$\vdots$

$(\alpha+(p-1))^p + (\alpha+(p-1)) + 3 = 0$

Number field (= Finite extension of $\mathbb{Q}$)

$[\mathbb{Q}(\sqrt{d}):\mathbb{Q}] = 2$, assume d is squarefree

(e.g., $\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$)

$\mathbb{Q}(\zeta_n) = \mathbb{Q}(e^{2\pi i/n})$

$[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n) = \#$ of integers $1 \le k \le n$ coprime to n.

Ex: Show $\mathbb{Q}(\sqrt{p}) \not\cong \mathbb{Q}(\sqrt{q})$ for distinct primes p, q.

$\mathbb{Q}(\sqrt{p})$ has a squareroot of p

But $\mathbb{Q}(\sqrt{q})$ does not

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

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

Then $a=0$ or $b=0$

So $a^2 = p$ or $b^2q = p$

which is a contradiction.

$\theta \in \mathbb{R}$. $F_\theta = \mathbb{Q}(\sin\theta)$

$E_\theta = \mathbb{Q}(\sin\frac{\theta}{3})$

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

Show $\sin\theta \in \mathbb{Q}(\sin\frac{\theta}{3})$

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

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

$3\cos^2\frac{\theta}{3}\sin\frac{\theta}{3} - \sin^3\frac{\theta}{3} = \sin\theta$

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

To understand $[E_\theta : F_\theta] = [F_\theta(\sin\frac{\theta}{3}) : F_\theta]$

$\stackrel{*}{=}$ degree of minimal polynomial of $\sin\frac{\theta}{3}$

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

$F(x)$ $x^n + a_{n-1}x^{n-1} + \dots = 0$

$F(x)$ spanned by $1, x, x^2, \dots, x^{n-1}$

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

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

$\Rightarrow [E_\theta : F_\theta] \leq 3$

E.g., $F = \mathbb{Q}$, $\theta = 0$, $F_\theta = \mathbb{Q}$, $E_\theta = \mathbb{Q}$, deg $= 1$

E.g., $F = \mathbb{Q}$, $\theta = \pi$, $F_\theta = \mathbb{Q}$, $E_\theta = \mathbb{Q}(\sin\frac{\pi}{3}) = \mathbb{Q}(\frac{\sqrt{3}}{2})$, deg $= 2$

E.g., $F = \mathbb{Q}$, $\theta = \frac{\pi}{6}$, $F_\theta = \mathbb{Q}$, deg 3 since

$x^3 - \frac{3}{4}x + \frac{1}{4}\cdot\frac{1}{2} = 0$ is irreducible

(check no rational roots, suffices to check finitely many possibilities using the rational root theorem)

Show that $\mathbb{Q}(t_1, t_2, \ldots, t_n)$ is isomorphic to a subfield of $\mathbb{R}$.

Idea: the $t_1, \ldots, t_n$ need to correspond to real numbers with no algebraic relations between them.

Pick $t_1 \in \mathbb{R} \setminus \underbrace{\overline{\mathbb{Q}}}_{\text{countable}}$

Pick $t_2 \in \mathbb{R} \setminus \underbrace{\overline{\mathbb{Q}(t_1)}}_{\text{countable}}$

$\vdots$

---

1) Show $G = GL(2, \mathbb{F}_{p^n})$ has order $(p^{2n}-1)(p^{2n}-p^n)$

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

---

1) $\left(\square, \square\right)$

$p^{2n}-1$ possibilities

$p^{2n} - p^n$

Can't be one of the p^n multiples of the first column

2) Amounts to checking that the subgroup

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \cong (\mathbb{F}_{p^n}, +)$$

check $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$

Check $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$

The field $\mathbb{F}_{p^n}$ has multiplicative group

$\mathbb{F}_{p^n}^\times$, cyclic of order p^n-1.

(Because $x^d = x$ has $\leq d$ solutions in $\mathbb{F}_{p^n}$,
and then some abstract group theory
says that $\mathbb{F}_{p^n}^\times$ must be cyclic)

(This is true for any finite multiplicative subgroup of a field (e.g., $\{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$))

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

---

0 has a squareroot,

$\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ half of these can be divided by 2.

$\mathbb{F}_p^\times \xrightarrow{x^2} \mathbb{F}_p^\times$ $\qquad 1 + \frac{p-1}{2}$.

$\mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{2x} \mathbb{Z}/(p-1)\mathbb{Z}$

Cuberoots

$\mathbb{Z}/(p-1)\mathbb{Z} \xrightarrow{3x} \mathbb{Z}/(p-1)\mathbb{Z}$

If $3 \mid p-1$, then $1 + \frac{p-1}{3}$

else, 3 invertible mod $p-1$, so all p elements have ~~squareroots~~ cuberoots

---

Show $[n \geq 2$ and $2^n + n^2$ prime$] \Rightarrow n \equiv 3 \pmod 6$

Two strategies: - Check divisibility by a small prime
- Or use an algebraic factorization (e.g., n^4+4 $=$ $(n^2+2n+2)(n^2-2n+2)$)

Here: Look mod 2 and mod 3.

$2^n + n^2 \equiv n^2 \equiv n \pmod 2$

So divisible by 2 unless $n \equiv 1 \pmod 2$.

$2^n + n^2 \equiv ? \pmod 3$

Since n odd,

$2^n \equiv 2 \pmod 3$

So divisible by 3 unless $n \equiv 0 \pmod 3$ (so $n^2 \equiv 0$, rather than $n^2 \equiv 1$)

n	$2^n \pmod 3$	$n^2 \pmod 3$
0	1	0
1	2	1
2	$4 \equiv 1$	$4 \equiv 1$
3	2	$3^2 \equiv 0^2 \equiv 0$
4	1	$4^2 \equiv 1^2 \equiv 1$
⋮		$5^2 \equiv 2^2 \equiv 1$

Combine CRT : $n \equiv 3 \pmod 6$

Euler's Theorem: If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod n$

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Ex: $17^{17^{17}} \pmod{10}$

$17^4 \equiv 1 \pmod{10}$ since $\gcd(17, 10) = 1$ and $\varphi(10) = 4$

so $17^{(17^{17})} \equiv 17^1 \pmod{10}$ since $17^{17} \equiv 1^{17} \equiv 1 \pmod 4$

$= 7 \pmod{10}$

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

$17^2 \equiv 7^2 \equiv 9 \pmod{10}$

$17^3 \equiv 3 \pmod{10}$

$17^4 \equiv 1 \pmod{10}$

$17^5 \equiv 7 \pmod{10}$

M real, symmetric

M positive definite $\iff$ Eigenvalues > 0

$\iff x^T M x > 0$ (same) for $x \neq 0$

$\iff \langle x, Mx \rangle > 0$

$\iff M = A^T A$ (note $(A^T A)^T = A^T A^{TT} = A^T A$ for A invertible)

M positive semidefinite $\iff$ Eigenvalues ≥ 0

$\iff x^T M x \geq 0$

M positive semi-definite $\iff$ Eigen...

$\iff x^T M x \geq 0$

$\iff \langle x, Mx \rangle \geq 0$

$\iff M = A^T A$ for some A.

strongest

use this if pos def is an assumption