Field F, finite subgroup $H \leq F$, then H cyclic.

Solution: $\rightarrow$ Extracting some group-theoretic info

$x^d - 1 = 0$ has at most d solutions in F

so $x^d = 1$ has at most d solutions in H

$\rightarrow$ Use characterization of cyclic groups

$\rightarrow$ We know that H has at most one subgroup of order d. So H cyclic

---

F characteristic $p > 0$, α a root of $f(x) = x^p - x + 3$ in an extension of F. Show $f(x)$ has p distinct roots in $F(\alpha)$.

Frobenius endomorphism

$F \to F$

$x \mapsto x^p$ ring homomorphism

$$(x+y)^p = x^p + \underbrace{\boxed{\binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1}}}_{\text{all div by } p} + y^p$$

$= x^p + y^p$ in char p

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

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

So $\alpha, \alpha+1, \dots, \alpha+p-1$ are p distinct roots in $F(\alpha)$

(or $f(\alpha+k) = (\alpha+k)^p - (\alpha+k) + 3$

$= \alpha^p + k^p - (\alpha+k) + 3 \underset{k^p \equiv k \pmod p}{=} \alpha^p - \alpha + 3 = 0$)

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

Show $F_\theta \subseteq E_\theta$, determine $[E_\theta : F_\theta] = \dim_{F_\theta} E_\theta$.

Solution:

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

$\downarrow$ imaginary part

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

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

- Then $F_\theta \subseteq E_\theta$
- $\sin\frac{\theta}{3}$ satisfies $\left.\begin{array}{l} -4x^3 + 3x - \sin\theta = 0 \\ 4x^3 - 3x + \sin\theta = 0 \end{array}\right\}$ has coefficients in F_θ

$\Rightarrow \dim_{F_\theta} E_\theta \leq 3$ (E_θ spanned by $1, \sin\frac{\theta}{3}, \sin^2\frac{\theta}{3}$)

$F_\theta = \mathbb{Q}(\sin 0) = \mathbb{Q}$, $E_\theta = \mathbb{Q}(\sin\theta) = \mathbb{Q}$

$\Rightarrow \dim_{F_\theta} E_\theta = 3$

$\theta = 0 \rightsquigarrow F_\theta = \mathbb{Q}(\sin 0) = \mathbb{Q}$, $E_\theta = \mathbb{Q}(\sin\theta) = \mathbb{Q}$, $\dim = 1$

$\theta = \pi \rightsquigarrow F_\theta = \mathbb{Q}(\sin\pi) = \mathbb{Q}$, $E_\theta = \mathbb{Q}(\sin\frac{\pi}{3}) = \mathbb{Q}(\frac{\sqrt{3}}{2})$ $\dim = 2$

$\theta = \frac{\pi}{6} \rightsquigarrow F_\theta = \mathbb{Q}(\sin\frac{\pi}{6}) = \mathbb{Q}$, $E_\theta = \mathbb{Q}(\sin\frac{\pi}{18})$.

we need to show $4x^3 - 3x + \frac{1}{2}$ irreducible$/\mathbb{Q}$.

rational root thm: $8x^3 - 6x + 1$ ....

check $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$.

F is a field of cardinality p^n, p prime, $n > 0$, $G = GL(2,F)$.

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

b) A sylow p-subgroup of G is isomorphic to $(F,+)$

Pf: $\begin{bmatrix} \bigcirc & \bigcirc \end{bmatrix}$

has $p^{2n}-1$ possibilities — has $p^{2n}-p^n$ possibilities

In general, for $k\times k$ matrices

$(p^{kn}-1)(p^{kn}-p^n)(p^{kn}-p^{2n}) \cdots (p^{kn}-p^{(k-1)n})$

b) All Sylow p-subgroups are isomorphic (because conjugate) Sylow's 2nd theorem
so enough to find one Sylow p-subgroup isomorphic to F

There are p^n matrices: $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cong \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$

$F \longrightarrow P$

$a \longmapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$.

In general, $\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ is a Sylow p-subgroup of $GL(k,F)$.

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

How many elements of $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$

are squares? — are doubles?

are cubes? — are triples?

What is im of $x \mapsto 2x$

are cubes:

What is |im| of $x \mapsto 2x$

What is |im| of $x \mapsto 3x$

For squares/doubles,
$|\mathrm{im}| = \frac{p-1}{|\ker|} = \frac{p-1}{|\{0, \frac{p-1}{2}\}|} = \frac{p-1}{2}$ $\left(p-1 \mid 2x, \ \frac{p-1}{2} \mid x\right)$

So $\frac{p+1}{2}$ total (unless $p=2$, in which case 2 total)

For cubes/triples:
$|\mathrm{im}| = \frac{p-1}{|\ker|} = \begin{cases} \frac{p-1}{|\{0, \frac{p-1}{3}, \frac{2(p-1)}{3}\}|} & \text{if } p \equiv 1 \pmod 3 \\ \frac{p-1}{|\{0\}|} & \text{if } p \equiv 2 \pmod 3 \end{cases}$ (Ignore $p=3$)

or $|\mathrm{im}| = p-1$ since multiplication by 3 mod $(p-1)$ is a bijection since $3 \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$.

Final answer $= \begin{cases} 3 & p=3 \\ 1+\frac{p-1}{3} & p \equiv 1 \pmod 3 \\ p & p \equiv 2 \pmod 3 \end{cases}$

$n \geq 2$, $2^n + n^2$ prime, show $n \equiv 3 \pmod 6$

Sol: Look at divisibility by $2 \Rightarrow n \equiv 1 \pmod 2$

(sometimes factorizations are helpful: $n^4+4 = (n^2+2n+2)(n^2-2n+2)$)

Look at divisibility by 3:

We know $2^n \equiv 2 \pmod 3$ (since $n \equiv 1 \pmod 3$, $2^2 \equiv 1 \pmod 3$)

so $n^2 \not\equiv 1 \pmod 3$

so $n \not\equiv 1,2 \pmod 3$

$n \equiv 0 \pmod 3$ $\longrightarrow$ CRT: $n \equiv 3 \pmod 6$

$A = 17^{17^{17}}$, determine $A \pmod{10}$

Sol: We know $17^4 \equiv 1 \pmod{10}$ (by Euler's Thm $a^{\varphi(n)} \equiv 1 \pmod n$ for $\gcd(a,n)=1$)

$(17 \in (\mathbb{Z}/10\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$
$\cong \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$\cong \mathbb{Z}/4\mathbb{Z}$

$17^{17^{17}} \equiv \underbrace{7^1}_{\equiv 7} \pmod{10}$ because $17^{17} \equiv 1^{17} \equiv 1 \pmod 4$

ϕ Euler's function, a, k integers, $a > 1$, $k > 0$.
show $k \mid \phi(a^k - 1)$.

Pf: We know $\phi(a^k-1) = |(\mathbb{Z}/(a^k-1)\mathbb{Z})^\times|$

a has order k in $(\mathbb{Z}/(a^k-1)\mathbb{Z})^\times$

Pf. We know $\phi(a^k - 1)$ ...

a has order k in $(\mathbb{Z}/(a^k-1)\mathbb{Z})^\times$

so $k \mid \phi(a^k-1)$.

Symmetric matrix A | A Pos def $\iff$ Eigenvalues > 0 $\iff$ $x^T A x > 0 \quad \forall x \neq 0$

$\langle x, Ax \rangle > 0$

$\iff$ $A = B^T B$, B invertible

A pos semidef $\iff$ Eigenvalues ≥ 0 $\iff$ $x^T A x \geq 0 \quad \forall x$

$\langle x, Ax \rangle \geq 0 \quad \forall x$

Over $\mathbb{R}$ (over $\mathbb{C}$, these transposes, need to be conjugate transposes) $\iff$ $A = B^T B$ (any B)

A, B real $n \times n$ symmetric matrices, B positive definite.

$$G(x) = \frac{\langle Ax, x\rangle}{\langle Bx, x\rangle} \quad \text{for } x \neq 0.$$

(Note: $\langle Bx, x\rangle > 0$ since B is positive def.)

a) G attains a maximum value

b) Show that any maximum pt u for G is an eigenvector for a certain matrix related to A, B.

Pf: a) We have
$$G(\lambda x) = \frac{\langle A\lambda x, \lambda x\rangle}{\langle B\lambda x, \lambda x\rangle} = \frac{\lambda^2 \langle Ax, x\rangle}{\lambda^2 \langle Bx, x\rangle} = G(x)$$

so the values of G are the same as the values of G on the unit sphere in $\mathbb{R}^n$.

Then (a) follows from extreme value theorem, continuity of G, compactness of sphere.

b) Write $B = C^T C$ for some invertible matrix C.

$$G(x) = \frac{\langle Ax, x\rangle}{\langle Bx, x\rangle} = \frac{\langle Ax, x\rangle}{\langle C^T C x, x\rangle} = \frac{\langle Ax, x\rangle}{\langle Cx, Cx\rangle}$$

$$\langle C^T C x, x\rangle = x^T C^T C x = (Cx)^T Cx = \langle Cx, Cx\rangle$$

Let $y = Cx$:
$$G(x) = \frac{\langle AC^{-1}y, C^{-1}y\rangle}{\langle y, y\rangle} = \frac{\langle C^{-T} A C^{-1} y, y\rangle}{\langle y, y\rangle}$$

Rayleigh's Thm:

$G(x) \leq \lambda_{max}$ of $C^{-T}AC^{-1}$

attained on any eigenvector y of $C^{-T}AC^{-1}$ with eigenvalue λ_{max}.

$\lambda_{min} \leq$ Rayleigh quotient of $C^{-T}AC^{-1}$ $\leq \lambda_{max}$

equality on eigenvectors with eigenvalues λ_{min}

extreme eigenvalues of $C^{-T}AC^{-1}$

... eigenvector of $C^{-1}C^{-T}A$)

eigenvalue λ_{max}. ... $_{min}$ eigenvalue of $C^{-T}AC^{-1}$.

(i.e., x eigenvector of $C^{-1}C^{-T}A$)

$B^{-1}A$

$$C^{-T}AC^{-1}y = \lambda y$$

$$C^{-T}AC^{-1}Cx = \lambda Cx$$

$$C^{-1}C^{-T}Ax = \lambda x$$

$$(C^TC)^{-1}Ax = \lambda x$$

$$B^{-1}Ax = x$$