① Suppose nontrivial $H \le G$ is contained in every nontrivial subgroup of G. Show $H \le Z(G)$.

<u>Proof:</u>/ We need to show that $Z(G)$ is nontrivial; then it follows.

Suppose $Z(G)$ <u>is</u> trivial. Since H is contained in every nontrivial subgroup, and $|gHg^{-1}| = |H|$, $H \le gHg^{-1} \Rightarrow H = gHg^{-1}$ $\forall g \in G$.

Thus H is normal in G.

$\boxed{\forall x \in G,\ H \le \langle x \rangle. \text{ As cyclic groups are abelian, } xh = hx\ \forall h \in H, \text{ thus } H \le Z(G).}$ ∎

② Let n be odd, and suppose $G \le S_n$ has order 2^k. Prove that $\exists i \in \{1, \dots, n\}$ fixed by all $\sigma \in G$.

$n =$ sum of sizes of G-orbits.

But, the size of each nontrivial G-orbit is a power of 2 by orbit-stabilizer: $|G(x)| = \frac{|G|}{|Stab_G(x)|}$

Since n is odd, there must be at least one orbit of size 1. ∎

③ Let p be an odd prime. How many elements can have square roots in $\mathbb{F}_p$? cube roots?

If $p = 3$, only 1:

$p = 5$: $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$ so 2 elems

- Multiplicative group is cyclic of even order $p-1$.

Consider $\varphi: \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^2$ which has kernel $\{\pm 1\}$, as $x^2 - 1$ has exactly 2 roots in $\mathbb{F}_p[x]$.

Then $\mathbb{F}_p^\times / \ker\varphi \cong \varphi(\mathbb{F}_p^\times)$ and $|\varphi(\mathbb{F}_p^\times)| = \frac{1}{2}(p-1)$ is the # of squares in $\mathbb{F}_p$.

Now consider $\psi: x \mapsto x^3$ which has as kernel the roots of $x^3 - 1 = (x-1)(x^2+x+1)$

If $3 \nmid p-1$, then $\ker\psi = 1$ and there are $p-1$ cubes in $\mathbb{F}_p$.

If 3 does divide $p-1$, then $\mathbb{F}_p^\times$ has an element of order 3, whose inverse has order 3, and there are thus $\frac{1}{3}(p-1)$ cubes as $|\ker\psi| = 3$. ∎

④ Let $W \le V$ be vector spaces of degree m, n respectively. Let $T: V \to V$ be a linear transformation s.t. $T(V) \subseteq W$. Let T_W be $T|_W$. Prove $\det(I_n - xT) = \det(I_m - xT_W)$.

<u>Solution:</u>/ • Note this is <u>not</u> asking about characteristic polynomials

(5) Let $F_\Theta = \mathbb{Q}(\sin\Theta)$ for some $\Theta \in \mathbb{R}$, $E_\Theta = \mathbb{Q}(\sin\frac{\Theta}{3})$.
Show that E_Θ is an extension of F_Θ and determine the possibilities for $[E_\Theta : F_\Theta]$.

$$\sin(\alpha \pm \beta) = \sin\alpha\cos\beta \pm \cos\alpha\sin\beta \qquad \cos(2\Theta) = 1 - 2\sin^2\Theta$$

$$\sin\Theta = \sin\left(\tfrac{\Theta}{3} + \tfrac{2\Theta}{3}\right) = \sin\tfrac{\Theta}{3}\cos\left(\tfrac{2\Theta}{3}\right) + \cos\left(\tfrac{\Theta}{3}\right)\sin\left(\tfrac{2\Theta}{3}\right)$$

$$= \sin\tfrac{\Theta}{3}\left(1 - 2\sin^2\tfrac{\Theta}{3}\right) + \cos\left(\tfrac{\Theta}{3}\right)\cdot 2\sin\tfrac{\Theta}{3}\cos\tfrac{\Theta}{3}$$

$$= \sin\left(\tfrac{\Theta}{3}\right)\left(1 - 2\sin^2\left(\tfrac{\Theta}{3}\right)\right) + 2\sin\tfrac{\Theta}{3}\left(1 - \sin^2\tfrac{\Theta}{3}\right)$$

This shows that $F_\Theta \subseteq E_\Theta$.

$[E_\Theta : F_\Theta]$ can be 1: $\Theta = \pi/2$ gives $F_\Theta = \mathbb{Q}$
and $E_\Theta = \mathbb{Q}(\sin\pi/6) = 1/2$

6. Let $g(x) = x^7 - 1 \in \mathbb{Q}[x]$, and let K be a splitting field for $g(x)$ over $\mathbb{Q}$.

(a) Show that $g(x) = (x-1)h(x)$ where $h(x)$ is irreducible in $\mathbb{Q}[x]$. (Hint: Study $h(x+1)$ by first writing $h(x) = g(x)/(x-1)$. Use Eisenstein's criterion to show $h(x+1)$ is irreducible.)

(b) Show that $G = \mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 6, and has as a generator the map that takes $\omega \mapsto \omega^3$ for any root ω of $g(x)$.

(c) Let ω be a complex 7^{th} root of 1. Let

$$x_1 = \omega + \omega^2 + \omega^4, \quad x_2 = \omega + \omega^6.$$

Find subgroups H_1, H_2 of G such that $\mathbb{Q}(x_1)$ is the fixed field of H_1 and $\mathbb{Q}(x_2)$ is the fixed field of H_2. Find $[\mathbb{Q}(x_1) : \mathbb{Q}]$ and $[\mathbb{Q}(x_2) : \mathbb{Q}]$.

(d) Show that $\mathbb{Q}(x_1)$ and $\mathbb{Q}(x_2)$ are the only fields M with $\mathbb{Q} \subset M \subset \mathbb{Q}(\omega)$. (Here $\subset$ denotes proper containment.)

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1

a) $g(x) = (x-1)(x^6 + \dots + x + 1)$.

$$h(x+1) = (x+1)^6 + (x+1)^5 + \dots + x + 1 + 1$$

$$= x^6 + \left(\binom{6}{1}+1\right)x^5 + \left(\binom{6}{2}+\binom{5}{1}+1\right)x^4 + \left(\binom{6}{3}+\binom{5}{2}+\binom{4}{1}+1\right)x^3$$

$$+ \left(\binom{6}{4}+\binom{5}{3}+\binom{4}{2}+\binom{3}{1}+1\right)x^2 + \left(\binom{6}{5}+\binom{5}{4}+\binom{4}{3}+\binom{3}{2}+\binom{2}{1}+1\right)x + 7$$

$$= x^6 + 7x^5 + 21x^4 + 35x^3 + 35x^2 + 21x + 7$$

so $h(x+1)$ is Eisenstein at 7, thus irreducible.

If $h(x)$ were reducible:
$h(x) = g(x)f(x)$ then $h(x+1) = g(x+1)f(x+1)$

b) If ω a primitive 7^{th} root
then any $\sigma \in G$ is determined by $\sigma_a(\omega) = \omega^a$.

$$\sigma_3^2(\omega) = (\omega^3)^3 = \omega^2$$
$$\sigma_3^3(\omega) = (\omega^2)^3 = \omega^6$$
$$\sigma_3^4(\omega) = (\omega^6)^3 = \omega^4$$
$$\sigma_3^5(\omega) = (\omega^4)^3 = \omega^5$$
$$\sigma_3^6(\omega) = (\omega^5)^3 = \omega$$

(c) If $x_1 = \omega + \omega^2 + \omega^4$, then $\mathbb{Q}(x_1)$ is the fixed field of σ_2

$$\sigma_2(\omega + \omega^2 + \omega^4) = \omega^2 + \omega^4 + \omega = x_1$$

σ_2 has order 3, so

$\mathbb{Q}(\omega)$	1
|	|
$\mathbb{Q}(x_1)$	H
| $[G:H]$	|
$\mathbb{Q}$	G

$[G : \langle\sigma_2\rangle] = 2$
so $[\mathbb{Q}(x_1) : \mathbb{Q}] = 2$.

If $x_2 = \omega + \omega^6$, then $\mathbb{Q}(x_2)$ is fixed by $\langle\sigma_6\rangle$.

$\sigma_6(\omega^6) = \sigma_6(\omega)^6 = \omega^{36} = \omega$ so $\sigma_6(\omega + \omega^6) = \omega^6 + \omega$.

This map has order 2 so $[\mathbb{Q}(x_2) : \mathbb{Q}] = 3$.

(d) Any intermediate field corresponds to a subgroup of G, but as G is cyclic of order 6, it has a unique subgroup of order 2 and of order ?.