(1) Assume G is an infinite nonabelian group whose proper subgroups are finite. Show that every proper normal subgroup of G is contained in $Z(G)$. Explain why $G/Z(G)$ is an infinite simple group whose proper subgroups are finite. ⟵ 4th isomorphism theorem?

Proof:/ Let $N \trianglelefteq G$. Then $\forall g \in G$, $gNg^{-1} = N$.

- If $N \nsubseteq Z(G)$, $\exists\, n \in N - Z(G)$ and $g \in G$ s.t. $gn \neq ng$. But then $gng^{-1} \in N - Z(G)$ and $gng^{-1} \neq n$, so $\exists\, g' \in G$ s.t. $g'(gng^{-1})(g')^{-1} \in N - Z(G)$ and $g'(gng^{-1})(g')^{-1} \neq n, \neq gng^{-1} \ldots$ Thus N cannot have been finite as we can proceed w/ this process infinitely. So, $N \subseteq Z(G)$.
- If $G/Z(G)$ had a normal subgroup, that would correspond to a normal subgroup of G containing $Z(G)$. Similarly, a proper infinite subgroup of $G/Z(G)$ corresponds to a proper infinite subgroup of G containing $Z(G)$.

(2) Suppose A_4 acts transitively on a set $\mathcal{X}$. What are possible sizes of $\mathcal{X}$?

$|A_4| = 12$, and since the action of A_4 on $\mathcal{X}$ is transitive, we have $\forall x \in \mathcal{X}$,
$|\mathcal{X}| = \frac{|A_4|}{|\mathrm{Stab}_{A_4}(x)|}$, so $|\mathcal{X}|$ divides $|A_4|$ and is thus one of $\{1, 2, 3, 4, 6, 12\}$.

But, $A_4 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4) \rangle$

Since A_4 can only permute up to 4 elements, $|\mathcal{X}| \in \{1, 2, 3, 4\}$.

(3) Let A be an integral domain containing a field F as a subring. This makes A a vector space over F.
Show if A is finite dimensional over F then A is a field, and show this need not be true if A is infinite dimensional over F.

Proof: – Let $F = \mathbb{Q}$ and $A = \mathbb{Q}[x]$. Then A is infinite dimensional over F but A is not a field.

If $\dim_F A = n$, then let $a_1, \ldots, a_n$ be a basis for A over F. We claim $A \cong F^n$.

Indeed, let $\varphi: F^n \to A$ be the map sending $(c_1, \ldots, c_n) \mapsto c_1 a_1 + \cdots + c_n a_n$.

φ is surjective as $a_1, \ldots, a_n$ are a basis for A over F,

and is injective since $c_1 a_1 + \cdots + c_n a_n = 0$ implies $c_1 = \cdots = c_n = 0$, and clearly φ is a homomorphism of F-modules.

(4) Let G be a group for which $\exists$ injective homomorphism $\alpha: \mathbb{Z}^n \to G$ and surjective homomorphism $\beta: \mathbb{Z}^n \to G$.
What are the possible isomorphism types for G?

– Since α is injective and β is surjective, we know that G is countable and infinite.

We can have $G \cong \mathbb{Z}^n$

↳ can we drop rank?

G is abelian: $x, y \in G$ are $\beta(a), \beta(b)$ for $a, b \in \mathbb{Z}^n$ and
$x + y = \beta(a) + \beta(b) = \beta(b) + \beta(a) = y + x$.

G is finitely generated: $a_1, \ldots, a_n$ generate $\mathbb{Z}^n$ so $\beta(a_1), \ldots, \beta(a_n)$ generate G.

objective hom from $\mathbb{Z}^2 \to \mathbb{Z}$?

↳ $\ker \alpha \neq \{(0,0)\}$

– Cannot combine factors or we lose injectivity.

This comes from the universal property of group products.

⑤ ⓘ $\mathbb{F}_3[x]/(x^2+1)$, ⓘⓘ $\mathbb{F}_3[x]/(x^2+2)$, ⓘⓘⓘ $\mathbb{F}_3[x]/(x^2+2x+2)$.

ⓐ Show each of the above rings is a product of fields and say which fields are involved

ⓑ For each pair of isomorphic rings, give an explicit isomorphism.

ⓘ x^2+1 is irreducible over $\mathbb{F}_3$, as it has no roots in $\mathbb{F}_3$ and is quadratic.

Elements look like $ax+b$, where $a,b \in \mathbb{F}_3$.

$$(ax+b)(cx+d) = (ac)x^2 + (ad+bc)x + bd$$
$$= ac(x^2+1) + (ad+bc)x + (bd-ac) \equiv (ad+bc)x + (bd-ac) \mod (x^2+1)$$

- Since x^2+1 is irreducible, (x^2+1) is a maximal ideal, thus $\mathbb{F}_3[x]/(x^2+1)$ is a field, and it is $\mathbb{F}_9$ since it is a field of degree 2 over $\mathbb{F}_3$.

ⓘⓘ x^2+2 has roots in $\mathbb{F}_3$: $x^2+2 = (x+1)(x+2)$

so by Chinese Remainder Theorem: $\mathbb{F}_3[x]/(x^2+1) \cong \mathbb{F}_3[x]/(x+1) \times \mathbb{F}_3[x]/(x+2) \cong \mathbb{F}_3 \times \mathbb{F}_3$

ⓘⓘⓘ x^2+2x+2 is quadratic with no roots in $\mathbb{F}_3$, so it is irreducible. Thus (x^2+2x+2) is a maximal ideal and $\mathbb{F}_3[x]/(x^2+2x+2) \cong \mathbb{F}_9$.

Elements look like $ax+b$

$$(ax+b)(cx+d) = acx^2 + (ad+bc)x + bd$$
$$= ac(x^2+2x+2) + (ad+bc-2ac)x + bd-2ac$$
$$\equiv (ad+bc-2ac)x + (bd-2ac)$$

ⓑ Isomorphism between $\mathbb{F}_3[x]/(x^2+1)$ and $\mathbb{F}_3[x]/(x^2+2x+2)$?

$ax+b \mapsto ax+(b-a)$
in $\mathbb{F}_3[x]/(x^2+2x+2)$

⑥ Let $p \geq 5$ be prime, and let L be the splitting field of x^p-1 over $\mathbb{Q}$.

ⓐ Find explicit generators for $Gal(L/\mathbb{Q})$. ⓑ Find generators for subfield $K \subseteq L$ s.t. $[L:K]=2$.

$L = \mathbb{Q}(\zeta)$, where ζ a p^{th} root of unity. The minimal poly of ζ is $x^{p-1} + \dots + x + 1$ and we have that any $\alpha_k \in Gal(L/\mathbb{Q})$ sends $\zeta \mapsto \zeta^k$ for $k \in \{1, \dots, p-1\}$.
since any of these are roots of the minimal polynomial.

So, $Gal(L/\mathbb{Q})$ is generated by $\{\alpha_k \mid k \in \{1,\dots,p-1\}\}$ and is cyclic since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

- Proving $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic: $(\mathbb{Z}/p\mathbb{Z})^\times$ is fin. gen. and abelian

so $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$ s.t. $1 | n_1 | n_2 | \dots | n_k$

- If $G = \langle \alpha \rangle$ and $d \,|\, |G|$, G has a subgp of order d with d elements of order dividing d.

As $n_k | n_i$ $\forall i$, each factor has n_k elements of order dividing n_k, and all these are distinct, so if $k>1$, $x^{n_k}-1$ has more than n_k roots in $\mathbb{F}[x]$.

ⓑ $Gal(L/\mathbb{Q})$ has a subgroup of order 2: $\langle \alpha_{-1} ; \zeta \mapsto \zeta^{-1} \rangle$.

Note $\zeta + \zeta^{-1}$ is in the fixed field of α_{-1}, so

$$\begin{array}{ccc} \mathbb{Q}(\zeta_p) & & 1 \\ \Big| \, 2 & \leftarrow & 2 \Big| \\ \mathbb{Q}(\zeta+\zeta^{-1}) & & Gal(L/\mathbb{Q}) \\ \Big| & & \Big| \\ \mathbb{Q} & & Gal(L/\mathbb{Q}) \end{array}$$