1. Let G be a finitely generated group (note that G need not be finite).

(a) Let G act by left-multiplication on the set G/H of left cosets of H. Compute the stablizer of the coset H.

(b) Let n be a positive integer. Show that G has only finitely many homomorphisms to the symmetric group S_n.

(c) Let n be a positive integer. Use the two parts above to show that G has only finitely many subgroups of index n.

(a) Let $G=\langle a_1,\dots,a_m\rangle$. Looking for $g\in G$ s.t. $gH=H$. But $gH=H$ iff. $g\in H$, so $\mathrm{Stab}_G(H)=H$.

(b) Since G is finitely generated, any homomorphism of G is completely determined by the image of its generators. Since there are $n!$ elements of S_n, there are at most $(n!)^m$ homomorphisms from G into S_n.

(c) A subgroup H of index n gives a homomorphism $\pi_H: G\to S_n$. Now, $x\in G$ belongs to H if and only if $xH=H$; that is, iff $\pi_H(x)(H)=H$. Thus H is completely determined by π. Since $\exists$ only finitely many homs into S_n, $\exists$ finitely many subgroups of index n. ∎

2. Suppose that $n=pq$ where p and q are primes such that $p\not\equiv 1 \pmod q$ and $q\not\equiv 1 \pmod p$. Show that there is only one group of size n, up to isomorphism. ← Only true if $p\neq q$. Else $\mathbb{Z}/p^2\mathbb{Z}\not\cong \mathbb{Z}_p\times\mathbb{Z}_p$

Let $|G|=n=pq$. Then G has Sylow subgroups P, Q of order p, q respectively that intersect trivially. WMA $q<p$. As $p\not\equiv 1 \bmod q$, $Q\trianglelefteq G$ so $G\cong P\ltimes_\varphi Q$ for $\varphi: P\to \mathrm{Aut}\,Q$. As Q is cyclic of prime order, $|\mathrm{Aut}(Q)|=q-1$.
Now $P=\langle a\rangle$ where $|a|=p$, and any $\varphi: P\to\mathrm{Aut}\,Q$ is determined by $\varphi(a)$.
Since $|\varphi(a)|$ divides $q-1$ and p, we see that $|\varphi(a)|=1$, so φ is trivial.
Thus, $G\cong P\times Q\cong \mathbb{Z}_p\times\mathbb{Z}_q$. ∎

3. Prove or disprove the following statement:

Every subring of $\mathbb{Q}[x]$ is a UFD (= unique factorization domain).

False: the subring of polynomials whose x coefficient is 0 is not a UFD.
↳ Closed under mult:
$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right)$$ the linear term has coefficient $a_0b_1+b_0a_1=a_0\cdot 0+b_0\cdot 0=0$

Claim x^2 is irred: $x^2=p(x)q(x)$. $\deg(p(x)q(x))=\deg p(x)+\deg q(x)=2$
Since neither has degree 1, w.m.a. $\deg p(x)=0$, so $p(x)$ is a unit from the field $\mathbb{Q}$.

x^3 is irred: If $\deg p(x)+\deg q(x)=3$ and neither has degree 1, one of $p(x), q(x)$ is a unit.

Then $x^6=x^2x^2x^2=x^3x^3$ has 2 distinct factorizations into irreducibles.

4. Let R be a ring. An R-module M is *projective* if whenever $h : A \to B$ is a surjective homomorphism of R-modules, and $g : M \to B$ is a homomorphism of R-modules, there exists a homomorphism $f : M \to A$ of R-modules, such that $h \circ f = g$. Use the definition itself directly to classify all cyclic projective modules over $\mathbb{Z}$.

$\mathbb{Z}$-modules are just abelian groups

$$\begin{tikzcd} M \arrow[d, "f"'] \arrow[dr, "g"] & \\ A \arrow[r, two heads, "h"'] & B \end{tikzcd}$$

Classify all cyclic projective $\mathbb{Z}$-modules:

M is cyclic if $\exists\, x \in M$ s.t. $M = \mathbb{Z}x$.

If M is cyclic then for the map $\pi(r) = rx$, $M \cong \mathbb{Z}/\ker\pi \cong \mathbb{Z}/(a)$

since $\mathbb{Z}$ is a PID.

$\mathbb{Z}$ itself is a cyclic $\mathbb{Z}$-module, and is projective. Is $\mathbb{Z}/(p)$ projective?

$$\begin{tikzcd} \mathbb{Z}/(p) \arrow[d] \arrow[dr, "g"] & \\ A \arrow[r, two heads] & B \end{tikzcd}$$

5. Find all irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$ explicitly.

– $f(x)$ cannot have a root in $\mathbb{F}_2$, and has nonzero constant term.

$x^4 + \_\, x^3 + \_\, x^2 + \_\, x + 1$ # of nonzero terms must be odd or 1 a root.

$x^4+1 = (x^2+1)^2 = (x+1)^4$

$x^4 + x^3 + 1$

• How can we get factoring as quadratics?

x^2+x+1 is the only irreducible quadratic. So if $f(x)$ has no roots in $f(x)$ but is still reducible, it is $(x^2+x+1)(x^2+x+1)$

$= x^4 + x^2 + 1$ is not irreducible.

so x^4+x^3+1, $x^4+x^3+x^2+x+1$

and x^4+x+1 are irreducible

6. Let p and q be distinct prime numbers and let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

(i) Show that the extension $K/\mathbb{Q}$ is Galois of degree 4.

(ii) Use the result of (i) to explicitly determine all the elements $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.

(i) We have that $[\mathbb{Q}(\sqrt{p}):\mathbb{Q}] = 2$ as $m_{\sqrt{p}}(x) = x^2 - p$.

Now as $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$, the minimal polynomial of $\sqrt{q}$ over $\mathbb{Q}(\sqrt{p})$ is $x^2 - q$, so

$[\mathbb{Q}(\sqrt{q},\sqrt{p}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{q},\sqrt{p}):\mathbb{Q}(\sqrt{p})]\,[\mathbb{Q}(\sqrt{p}):\mathbb{Q}] = 2 \cdot 2 = 4$

(ii)