Review of core topics from Algebra:

Pt 1: Groups

- Definitions: subgroups, subgroup test
- Examples:
  - cyclic groups
    key facts: • Isomorphic to $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.
    • $\forall\, d \mid n$, $\exists!$ subgp. of order d.
    (subgroup lattice is "E-T", useful in Galois).
    • (Also for general groups): $|g| = n$
    $\Rightarrow |g^m| = \frac{n}{(n,m)}$. $\rightsquigarrow$ determine # of generators of a cyclic gp.
  - $(\mathbb{Z}/n\mathbb{Z})^\times$ group under mult.,
    has size $\varphi(n)$, determined by prime power values.
    $\varphi(p^n) = p^n - p^{n-1}$.
    $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if n is prime.
    more general: finite subgp. of mult. gp. of a field is cyclic
  - Dihedral groups: $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$.
    many examples boil down to these relns,
    tracking what happens to vertices $1, 2$.
  - Symmetric group S_n, special sets of generators prove
    Cycle decompositions (unique up to reordering)
    make it easy to determine orders (lcm of sizes),
    inverses (write cycles in backwards order),
    ↗ Cycle types corr. to conj. classes!
    disjoint cycles commute. Sign map $\rightsquigarrow$ A_n ($A_{\geq 5}$ simple)

key ideas: homomorphisms, isomorphism theorems, kernel/image
(work have for rings, modules too.)
cosets/quotient groups, by normal subgps: often use projection $G \twoheadrightarrow G/N$.
Bijection b/w cosets $\rightsquigarrow$ Lagrange's Theorem.
Terminology: conjugation, normalizer, centralizer, center.

Fact: $H, K \leq G$, then $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$, $HK \leq G \iff HK = KH$.

Reformulating many things: Group actions:

Def: Stabilizers, orbits, kernel

Orbit-stabilizer theorem: $|\mathrm{Stab}(x)| \cdot |\mathrm{Orb}(x)| = |G|$

$G \curvearrowright X$ $[G : \mathrm{Stab}(x)] = |\mathrm{Orb}(x)|$. $\forall x \in X$.

Important gp actions:

- Conjugation (different sorts): Ex: $G \curvearrowright G$.

orbits are conj. classes, stabilizers are centralizers, orbits partition X.

$\rightsquigarrow |G| = \sum [G : C_G(g_i)] + |Z(G)|$

(reps of non-trivial conj. classes; conj. class of elt in center is a singleton)

App: p-groups (case power of prime p) have non-trivial center; iff: $p^n = \sum_{\text{pos. powers of } p} (\text{powers of } p) + |Z(G)|$.

Ex: Groups of size p^2 are $\mathbb{Z}_p$, size $p^2 \Rightarrow$ center $= p$ or p^2

if p^2, is abelian $\Rightarrow \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$ by Fund. Thm

else center has size $p \Rightarrow |G/Z(G)| = p \Rightarrow G/Z(G) \cong \mathbb{Z}_p$

(index is p, smallest prime divisor of $|G|$) $\Rightarrow$ normal.

is cyclic. $\Rightarrow G$ is abelian.

- $G \curvearrowright G$ by left mult. (left regular action)

$\rightsquigarrow$ Cayley's Theorem: $G \hookrightarrow S_n$. Can also do $G \curvearrowright H$, $H \leq G$.

App: Prove this. Another group of order 30 have normal 3,5-Syl

Key facts: Actions of G on A corr. to hom. $G \to \mathrm{Sym}(A)$ ≅ permutation rep.

Terminology: Transitive, faithful, kernel, orbit-stab $\rightsquigarrow$ Burnside's (counting)

And, of course, the Sylow Theorems! Be good at solving. numerical examples of these
Applying various group actions!

key results: classifying direct, semidirect products.

Ex: Groups of order $p \cdot q$, $p \neq q$ primes, $p<q$ (WLOG).
There's the cyclic one, $\mathbb{Z}_{pq}$, if $q \not\equiv 1 \pmod p$, that's it.
why: Cauchy $\rightsquigarrow \exists$ elts of order p, q, giving subgps P, Q
$[G:Q] = p$, smallest prime $|G| \Rightarrow Q \trianglelefteq G$, $|PQ| = \frac{|P||Q|}{|P \cap Q|} = |G|$ order pq
$\Rightarrow P, Q$ complements $\Rightarrow G \cong Q \rtimes_\varphi P$, some $\varphi: P \to \mathrm{Aut}(Q)$ by Lagrange
$\mathbb{Z}_p \cong \mathrm{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}/(q-1)\mathbb{Z}$
Only nontrivial exists if $p \mid (q-1)$ as orders of elts. divides in hom.
And we can recognize different φ giving iso. semidirect prods.

Fund. Thm of finitely gen. ab. grps: know how to
write inv. factors, elem.. divisors, convert b/w the two.
(esp: CRT).

Pt 2.
Rings Ex: Matrix rings, $\mathbb{Z}$ rings, poly, power series rings, $\mathbb{Z}[i] \leq \mathbb{Q}(i)$
Terminology: zero divisors, units ($\text{set} = R^\times$).
e.g.: $\mathbb{Z}_n^\times = \{0 \leq m \leq n-1 \mid (m,n)=1\}$.

int domain: comm. ring, $1 \neq 0$, no zero-divisors

Facts: homomorphisms, isomorphism theorems similar to grps,
ideals: subring $I \leq R$, closed under left/right mult. by elts of R.
can quotient by ideals,
$I+J$ = set of sums, IJ = finite set of sums of products.

Ex: ideal gen. by $a_1, \ldots, a_n$ is $(a_1, \ldots, a_n)$.

Fact: R comm, $R \neq 0$ field $\iff$ (0), (1) only ideals.
(thus, field hom. are either trivial or embeddings)

Max^{nl} ideals (no proper ideal "above it"), prime ideals ($P \neq R$, $ab \in P \Rightarrow a \in P$ or $b \in P$).

Facts: In a rng w/ 1, every proper ideal is in a max^{nl} ideal.

Recall: M max^{nl} ideal $\iff$ R/M a field.
P prime ideal $\iff$ R/P is and. int. domain

Cor: If R is comm, max^{nl} $\Rightarrow$ prime.

Key construction: Rings of fractions:

R comm, $\emptyset \neq D \subseteq R$,
$0 \notin D$, no 0-divisors in D, closed under mult.
form fractions, identify, do arithmetic as "expected"
$\rightsquigarrow$ ring where elts of D are units.

Ex) field of fractions of an intdomain: $FF(\mathbb{Z}) = \mathbb{Q}$,
$FF(\mathbb{Z}[i]) = \mathbb{Q}(i)$
$FF(\mathbb{Z}[x]) = \mathbb{Q}(x)$

Chinese Remainder Th^m: $A_1, \dots, A_k$ ideals in R, comm. w/ 1 $\neq 0$.
If A_i, A_j comax^{nl} $\forall i \neq j$, then

$$R/(A_1 \cdots A_k) = R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \cdots \times R/A_k$$

(slightly more general)

Ex: $(m,n) = 1_{\mathbb{Z}} \Rightarrow \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
"taking units $\Rightarrow$ Euler φ is mult.

IV

key examples of int. domains:

Euclidean domains: $\exists$ norm on R s.d.:

or $\forall a,b \in R$, $b \neq 0$, $\exists q, r \in R$: $a = qb + r$, $r = 0$ or $N(r) < N(b)$

$\rightsquigarrow$ Euclidean algorithm.

Ex: $\mathbb{Z}$ ($N(a) = |a|$), fields, ($r = 0$)

$F[x]$ for a field F.

$\mathbb{Z}[i]$ (geometric argument).

Have gcds and can compute via Euc. Alg.

PID: All "I" are "P" (principal).

Still have gcds! $(a,b) = (d)$.

not always easy to compute!

Fact: PID means non-zero primes are max^{al}.

UFD: primes: (p) is a prime ideal.

irred: r not 0 or a unit, $r = ab \Rightarrow a$ or b is a unit.

primes are always irred. converse true (for non-zero elts) in a PID

UFD means every non-zero, non-unit has a factorization into irreducibles, unique up to associates, reordering.

By Th^{m}: ED $\Rightarrow$ PID $\Rightarrow$ UFD.

Ex: $\mathbb{Z}[\sqrt{-5}]$ not a PID; as is not a UFD!

Factorize $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Check irreducibles here using norm map: $N(a+b\sqrt{-5}) = a^2 + 5b^2$

Fact: In a UFD, prime $\Leftrightarrow$ irred.

Gauß' Lemma: R = UFD, $F = FF(R)$, $p(x) \in R[x]$

then p red. in $F[x] \Rightarrow p$ red. in $R[x]$

If gcd of coeffs of $p(x) = 1$, then (e.g. monic poly) p irred in $R[x] \Leftrightarrow p$ irred. in $F[x]$

Th: R UFD $\Leftrightarrow R[x]$ UFD.

Cor: R UFD $\Rightarrow R[x_1, \dots, x_n]$ UFD.

Irreducibility criterion: deg. 2 or 3 over field

pol. f is irred. $\Leftrightarrow$ has a root in F.

; Rational roots Th: Good for UFDs (e.g. $\mathbb{Z}$, $\mathbb{Q}$).

Field of fract.

- Find $\not\Rightarrow$ irred. mod some prime (in $\mathbb{Z}_p[x]$).
(not always sufficient).

Eisenstein Criterion: R domain, P prime,

$f = x^n + c_{n-1}x^{n-1} + \dots + c_0$ monic, $n \geq 1$,

$c_0, \dots, c_{n-1} \in P$, $c_0 \notin P^2 \Rightarrow f$ is irred/R

(s. (F by Gauß).

Can also shift first: ex: cyclotomic pol: $\Phi_p(x) = \frac{x^p - 1}{x - 1}$,

$x \to x+1$.

Prop: F a field, $F[x]/(p(x))$ is a field $\Leftrightarrow p(x)$ is irred/F.

Suggested problems: (Groups/rings).

1). Let H be the subgroup of S_6 generated by (16425) and $(16)(25)(34)$. Let H act on Σ by conjugation. Show that the set

$$\Sigma := \{(12)(35)(46), (13)(24)(56), (14)(25)(36), (15)(26)(34), (16)(23)(45)\}$$

is invariant under this action, and thus we have a homomorphism $\varphi: H \to S_5$. Show that φ is an isomorphism.

2). Show that every group is a subgroup of a simple group.

3). Show that a group of order 300 cannot be simple.

4). For a commutative ring R, we say x is nilpotent if $\exists\, k \geq 1$ s.t. $x^k = 0$. Let P be the set of nilpotent elements. Show that P is an ideal, and that R/P has no nilpotent elements.

5). Let $R := \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{5}) =: F$.

Note that F is the field of fractions of R. Show:

1). $x^2 + x - 1$ is irreducible in $R[x]$, but not in $F[x]$.

2). R is not a UFD.

6). a). Show that $F := \mathbb{Z}_3[x] / (x^3 + x^2 + 2)$ is a field.

b). Find the multiplicative inverse of $x^2 + 1$ in F.