Final Review

Mark

Groups

Tools

$\varphi(n)$, **Euler's Phi Function**, "totient function," is the number of natural numbers $a \leq n$ such that $(a, n) = 1$

$$\boxed{\varphi(ab) = \varphi(a)\varphi(b) \text{ if } (a, b) = 1}$$

$$\boxed{\varphi(p^a) = p^a - p^{a-1} \text{ for prime p}}$$

p^a candidates
$\frac{p^a}{p} = p^{a-1}$ are divisible by p
(10/2 yield # numbers $\leq$ 10 divisible by 2)

example: $\varphi(15) = \varphi(5)\varphi(3) = 4 * 3 = 12$, since gcd(3, 5) = 1.

Fun: **last digit** of a number is the remainder when dividing by 10, aka mod 10 (for last three digits use mod 1000)

To compute a^{-1} **mod n**: For gcd(a, n) = 1, use euclidean algo, to find ax + ny = 1, meaning ax = 1 mod n. Thus, x is a^-1

Dihedral D_{2n}, Z_n and S_n

D_{2n}

The **elements** of D_{2n} are $\{1, r, ..., r^{n-1}, s, sr, ..., sr^{n-1}\}$.

Orders of elements are $|s| = |sr^i| = 2$ and $|r| = n$

Property: $r^i s = sr^{-i}$

D_{2n} can be described by

$$\langle r, s : r^n = 1 = s^2, rs = sr^{-1} \rangle$$

Which elements commute with all of D_{2n}? (aka center)

$$Z(D_{2n}) = \begin{cases} 1 & \text{for } n \text{ odd} \\ 1, r^{n/2} & \text{for } n \text{ even} \end{cases}$$

Symmetric Groups, S_n

Permutations of $\{1, 2, 3, ..., n\}$
each **uniquely** written as a product of disjoint cycles
idea of proof is to write any permutation $(a_1, ..., a_n)$ by closing once a loop is reached; this is guaranteed to happen since permutation is a bijective function!
order, $|S_n| = n!$

- **cycle order** is the **lcm** lengths of disjoint unique cycles
- an element has **order p**, prime, in S_n if and only if its cycle decomposition if a **product of p-cyles**. from homework, section 1.3 problem 14

*least common multiple is found by writing down the multiples of two numbers and finding the first common match.

can think of any permutation in S_n as acting on polynomial:

$$S_4 : (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

(123) sends x_1 to x_2 and so on; then, rewrite so each subscript $i < j$.

If, (-1) is present, the permutation is **odd**.
Sign of (12) is -1; sign of (123) is 1.

Conjugating in S_n

$\sigma = (12)(345)(6789)$ and $\tau = (1357)(2468)$,

$$\tau\sigma\tau^{-1} = (\tau(1)\tau(2))(\tau(3)...) = (3\ 4)(5...$$

hence two elements are conjugates only if they have the same cycle type.

Any element of S_n can be written as a **product of 2-cycles** (not uniquely!!) Whether the number of transpositions is odd or even, though, is unique!

Alternating, A_n

set of even permutations

$$|A_n| = \frac{n!}{2}$$

A_n is simple for all $n \geq 5$.

A_n is the kernel of $\varphi : S_n \to \{\pm 1\}$

S_5 is not solvable (by looking at composition series)

Curiosities
Fermat's Little Theorem: $a^p \equiv a$ mod p

Cyclic, Z_n

$Z_3 = \{0, 1, 2\}$ is a group with + mod 3

What are the **generators**? find a generator $< a >$,
all others are $< a^i >$ such that $(i, n) = 1$
example: $Z_8 =< 1 >=< 3 >=< 5 >=< 7 >$

For $|a| = n$,

$$|a^k| = \frac{n}{(n, k)}$$

What are **subgroups** of Z_n? subgroups are $< a^i >$ for each i a divisor of n
else, i is relatively prime, hence generates entire group

How many elements of order k in Z_n?

$$\varphi(k), \text{ if } k|n$$

elements of order k generate a cyclic group of order k.
Thus, the number of generators is $\varphi(k)$.

Isomorphisms

To show two groups are not isomorphic consider:

- abelian?
- elements have the same orders

For φ a homomorphism,

$$\text{Ker } \varphi = 1 \iff \varphi \text{ is } \textbf{injective}$$

Curious isomorphic groups: $D_6 \cong S_4$

Precisely 2 groups of order 4: V_4 and Z_4

Exercises

1. How many 3-cycles in S_4?

   $$(a\ b\ c)$$

   count options for $a * b * c = 4 * 3 * 2$, which can be written in 3 ways.
   So, total is $\frac{4*3*2}{3} = 8$

2. Elements of order 8 in $Z_{8,000,000}$?
   there are only 4 elements, since $\varphi(8) = 4$
   Note, $< 1m >$ is an element of order 8.
   Thus, the others $< 1m >$ raised to 3, 5, 7 (relatively prime to 8)

3. Find the lattice of Z_{p^2q} subgroups: $Z_p, Z_q, Z_{p^2}, Z_{pq}$

4. Number of divisors of 45?
$$45 = 3^2 5$$
divisors = (2+1)(1+1) = 6
(add 1 to powers and multiply)

5. For A, B subgroups of G, $A \cap B$ is a subgroup too.

6. Show σ^2 is even for all permutations σ look at the $\varphi : S_n \to \{\pm 1\}$; $\varphi(\sigma^2) = \varphi(\sigma)^2 = 1$, thus σ^2 is in the kernel of φ hence in A_n.

7. Show S_n is generated by $\{(1 \;\; i) : i \leq n\}$.
every permutation can be written as a transposition; use fact that $(ij) = (1\ i)(1\ j)(1\ i)$.

*to check homomorphism it sufficies to check generators and relations are preserved

$GL_n(F)$: set of all invertible (det$\neq 0$) with entries $\in F$, a field.

Quotient Groups

Cosets

For $H \leq G$,
cosets of H (gH for $g \in G$) **partition** G, each containing the same number of elements.

e.g., $\mathbb{Z}/\nvDash\mathbb{Z}$ partitions the integers into three cosets.

How?
Notice,
1. If $a \in bH$, $aH = bH$.
For all $x \in aH$, $x = ah_1 = bh_2h_1$
$\rightarrow x \in bH$.

2. aH, bH are disjoint or precisely the same.
Suppose $x \in aH \cap bH$. Then,
$x = ah_1 = bh_2$
$\rightarrow a \in bH$
Thus, $aH = bH$.

3. Every element of G is in some coset.
trivially, aH, for any $a \in G$.

4. $|H| = |aH|$ for any $a \in G$.
consider function f(h) = ah, for any $a \in G$.
f is bijective, meaning all cosets have the same number of elements.

Lagrange: for $H \leq G$,

$$|G| = |H| \ [G : H]$$

The **order** of any **element** has to divide the order of the group.
consider subgroup generated by the element, whose order then has to divide that of G.

Any **group of prime** order is cyclic (any element generates entire group).

Any group of order $2p \cong Z_{2p}$ or D_p
(Z_{2p} if it contains an element of order $2p$)

Normality

Can cosets be a group?

For $H \leq G$, define operation: $aHbH = abH$ (for $a, b \in G$).
*operation is on cosets

Key question: when is $aHbH = abH$ well-defined?

need to check whether two representatives from a coset, say a and a' (and b, b'), produce the same result under the operation.
Does $aHbH = a'Hb'H$?
If gHg^{-1}, then yes!

precisely when $H \trianglelefteq G$.

Thus, a subgroup N is **normal** in G if

$$gNg^{-1} \in N \text{ for all } g \in G$$
$$\text{equivalently, } gNg^{-1} = N$$

A subgroup with **index 2** is normal only two cosets reasoning...

An **element of order 2** a,

$$< a > \trianglelefteq G \iff a \in Z(G)$$

$< a > \trianglelefteq G$, so
xax^{-1} is e or a
can't be e if $a \neq e$.

If $G/Z(G)$ is cyclic, G **is abelian**. section 3.1 problem 36

Exercises

1. Show $H = < (1\ 2) > \leq S_3$, but not normal.
   If $H \trianglelefteq S_3$, then
   $$N_{S_3}(H) = S_3.$$
   But,
   $$(13)(12)(13)^{-1} = (23) \notin H$$

2. Show S_4 has no normal subgroup of order 8
   Suppose $H \trianglelefteq S_4$ with $|H| = 8$.

Then, S_4/H has order 3, meaning

$$(gH)^3 = H, \text{ for all } g$$

thus, $g^3 \in H$ for all $g \in G$.
all elements of order 2 raised to the third are themselves; thus, all elements of order 2 are in H, too many.

3. If $G/Z(G)$ is cyclic, show G is abelian. Let $xZ(G)$ be a generator of $G/Z(G)$ for some $x \in G$.
   Then for $a, b \in G$,
   $a = x^n c_a$ for some $c_a \in Z(G)$
   $b = x^m c_b$
   Since c_a, c_b commute with any element, $ab = x^n c_a x^m c_b = ba$.

Cauchy's Theorem

p divides the order of G, then G has an element of order p. proof later

HK in G

note HK need not be a subgroup; when is it?

$$H, K \leq G \text{ and } K \trianglelefteq G, \text{ then}$$
$$HK \leq G$$
$$e \in HK.$$
$$\text{For } a = h_1k_1 \in HK, \text{ a}^{-1} = k_1^{-1}h_1^{-1} \in HK$$

a set A **normalizes** K if it's a subset of $N_G(K)$.

What's the order of HK?

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

For H, $K \leq G$,

$$HK \textbf{ is a subgroup} \iff HK = KH.$$

If $H, K \leq G$, finite, with relatively prime orders,

$$H \cap K = 1$$

(problem 8 section 3.2) proof: look at orders of elements in H and K

Isomorphism Theorems

For φ a homomorphism:

$$\varphi : G \to H$$

Fundamental Homomorphism

$$G/Ker(\varphi) \cong \varphi(G)$$

"cosets of ker isomorphic to image"

Diamond Iso

$A, B \leq G$ and $A \trianglelefteq N_G(B)$

$$\begin{array}{ccc} & AB & \\ \text{A} & & \trianglelefteq B \\ & \trianglelefteq A \cap B & \end{array}$$

$$AB/B \cong A/(A \cap B)$$

Lattice Iso

$N \trianglelefteq G$

The structure of the subgroups of G/N is exactly the same as the structure of the subgroups of G containing N, with N collapsed to the identity element.

"G/N is all subgroups of G above N in lattice."

Composition Series

For a group G, construct

$$1 \leq N_1 \leq N_2 \leq ... \leq G$$

with $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is **simple**

*simple: no non-trivial normal subgroups
Then,

each N_{i+1}/N_i "composition factor" is **unique**

as is the number of N_i

*factorization is not necessarly unique

G **is solvable** if each N_{i+1}/N_i is abelian.
*N_{i+1}/N_i need not be simple

Group Actions

a group G **acting** on a set A is

Two conceptions:

operation such that
a) $1a = a$
b) $g_1 g_2 a$ is assocaitive

a **homo map** $G \to S_{|A|}$ (from G to the **symmetries** of A).

an action if **faithful** if its kernel is the identity

Conjugates of an element

There is a 1-to-1 correspondence between

conjugacy class of $a* \in G$
and
cosets of $C_a(G)$ (centralizer of a in G)

Note $xax^{-1} = yay^{-1} \iff xC_a(G) = yC_a(G)$
since this implies $y^{-1}x \in C_a$
Consider $f : xC_a \to$ conjugate of a, defined

$f(xC_a) = xax^{-1}$
injective: by above.
surjective: for any yay^{-1}, there is yC_a producing it.

Thus, number of conjugates of a equals the index of C_a in G.

$$\boxed{\text{conjugates of a} = [\text{G:C}_a]}$$

*conjugacy class** of a means the set xax^{-1} as x ranges over G.

Class Equation

see chp 24 in Gali For $H \leq G$,
there is a 1-to-1 correspondence between

conjugates of H
and
cosets of N

$\boxed{\text{note, for } a \in N(H), aHa^{-1} = H}$
$aHa^{-1} \subseteq H$
since for $h \in H$, $aha^{-1} \in H$.
$H \subseteq aHa^{-1}$
since aHa^{-1} contains as many elements as H
why?

By previous result, **number of conjugacy classes**

= size of orbits = index of stabilizer
= index of normalizer.

(for any element, the number of conjugates = index of its centralizer)

$$|G| = |Z(G)| + \text{ sum elements in each conjugacy class}$$

Orbits

Orbit of $a \in A$ by is $\{ga : g \in G\}$.
"Hit a with all $g \in G$", "spin a"

Orbits create **equivalence classes** in A

$$G_a = \textbf{stabilizer} \text{ of } a \text{ in } G$$

"elements of G such that $ga = a$"

$$\boxed{\text{size of } Orb(a) = [G : G_a]} = \text{ different } g\{G_a\}$$

$$= \text{index of stabilizer}$$

Ker of action on set aH "coset" = largest normal subgroup of G contained in H

Cayley's Theorem

any finite group G is isomorphic to a subgroup of S_n.

Consider function, $\pi_a(x)$ for $a \in G$ by ax. This function is bijective, hence permutes G. Therefore, we consider composition of functions π to see the permutations form a subgroup of S_n.

For p **the smallest** prime dividing $|G|$,

any subgroup of index $p \trianglelefteq G$.

Fundamental Theorem of finitely generated abelian groups

"FTFGAG"

every FGAG is the direct product of cyclic groups

$$\text{aka, } G \cong \underbrace{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}_{r} \ldots \underbrace{\frac{\mathbb{Z}}{n\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{n\mathbb{Z}}}_{invariant}$$

$$\text{invariants: } n_1 | n_2 \ldots | n_k$$

r is called **rank**

invariant factors are unique

recall,

any cyclic group is isomorphic to:

- $\mathbb{Z}$ is $(\mathbb{Z}, +)$ which is infinite

or

- $\frac{\mathbb{Z}}{n\mathbb{Z}}$ over $+$ is finite

So, $r = 0$ if G is finite.

Two FGA groups are **isomorphic $\iff$ same rank and invariant factors**

e.g., $|G| = 8$
possible expression as cyclic groups:
$\frac{\mathbb{Z}}{8\mathbb{Z}}$

$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}$
$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

Chinese Remainder Theorem

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$
$$\iff$$
$$(m, n) = 1$$

Traditionally written as $x \equiv a \mod n$ and $x \equiv b \mod m$ implies there is only one solution to $x \mod mn$. direct congruence proof

Hence, any group G can also be written in elementary divisor form:

$$G \cong \mathbb{Z}^r \times \prod \frac{\mathbb{Z}}{p_i^\alpha \mathbb{Z}}$$

*elementary divisors are not invariant factors!
* $Z_2 \times Z_2 \neq Z_4$ (different invariant factors)

Sylow's Theorem

G has order $p^\alpha m$, with p not dividing m, then G has a subgroup of order p^α.
Further,

- any 2 sylow p-groups are conjugate
- n_p the number is Sylow p-groups: $n_p \equiv 1$ mod p and $n_p | m$

- a unique Sylow p-group is **normal**

For $|G = 5 * 7|$, often **useful** to consider

quotients: G/P_7 (G mod a Sylow 7-subgroup)

subgroup: $H = P_7 P_5$

Exercises

1. Show G with $|G| = pq$ is cyclic
   number of Sylow p groups: $n_p \equiv 1$ mod p and $n_p | q$
   $\rightarrow n_p = 1$
   Similarly, $n_q \equiv 1$. Thus, the unique p and q subgroups are abelian, as they're of prime order.
   Further, both are normal $\rightarrow$ commutes.

2. Determine groups of order 99
   unique Sylow 11-subgroup and Sylow 3-subgroup. Thus, can show group is abelian, hence is Z_{99} or $Z_3 \times Z_{33}$

3. Find the invariant factors of all abelian groups of order $270 (= 2 * 3^3 * 5)$

   First find elementary divisors:

   $$Z_2 \times Z_{3^3} \times Z_5$$

   $$Z_2 \times Z_3 \times Z_{3^2} \times Z_5$$

   $$Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_5$$

   Then, for each abelian group, write powers in descending order:

p=3	p=2	p=5
3^3	2	5
1	1	1
1	1	1

   Each row yields an invariat factor. Here it's: Z_{270}

   For

   $$Z_2 \times Z_3 \times Z_{3^2} \times Z_5$$

   ,

p=3	p=2	p=5
3^2	2	5
3	1	1
1	1	1

the invariant factors are $Z_{90} \times Z_3$.

4. G with $|G| = 105$ has a normal Sylow 5-subgroup
   105 = 3*5*7 so
   $n_5 \equiv 1 \bmod 5$ and $n_5 | 3 * 7$
   meaning $n_5 = 21$ or 1...

Rings

an **abelian group** with multiplication such that

- * is associative and closed
- Distribution

a ring with multiplicative inverses (for non-zero elements) is called a "Division Ring" (or Skew field)

*field is a commutative division ring

u is a **unit** of R if there exists v such that $uv = vu = 1$.
u is a **zero divisor"** if there exists v such that $uv = 0$ or $vu = 0$.

In $\mathbb{Z}/n\mathbb{Z}$ an element is a unit (if relatively prime to n) or a zero divisor.

R^* is the set of all units of R.

an **Integral Domain** Ring is a ring with

- unit
- commutative
- no zero divisors

e.g., $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$ if n is prime

Quotient Rings

a ring **homomorphism** φ preserves + and *

Ker(φ) = elements mapping to 0

Ideals

analogous to normal subgroups. a subgring I is an **ideal** of R if

$$ir \in I \text{ and } ri \in I \quad \text{for all r } \in R \text{ and } i \in I$$

Thus, we defined a **quotient ring** as sets $r + I$, for r in ring with operations:

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I \text{ and } (r_1 + I) * (r_2 + I) = (r_1 r_2) + I$$

any ideal I is the **Ker** of homo $\varphi(r) = rI$.

Ker of φ is always an ideal.

prototypical example of ideal: $\mathbb{Z}$ with ideals $n\mathbb{Z}$

For I, J ideals of R,

- $I \cap J$ is an ideal
- IJ is defined as { finite sums ij}

only ideals of a field are trivial
for $a \in I$, there is $a^{-1} \in F$, so that $1 \in I$.

Lattice Isomorphism also preserves ideals between ring and quotient.

Special Ideals

an ideal is **principle** if it's generated by **one element**.
(using both + and *)

For R a commutative ring with unit,

an ideal M is **maximal** in R if

no other proper ideal contains M

$$\boxed{M \text{ is maximal } \iff R/M \text{ is a field}}$$

R/M is field means no ideals; by lattice iso, no ideals between R and M

(again assume commutative ring with unit)

a proper ideal is **prime** if $ab \in P$, then a or $b \in P$.

$$\boxed{\text{P is a prime ideal } \iff R/P \text{ is an integral domain}}$$

apparently follows from def, but unclear

Thus, max ideal $\rightarrow$ prime ideal (filed is an integral domain)

*monic polynomial means leading coefficient is 1

Finite Fields

For $p(x)$ **irreducible** in $F[x]$,

$$\boxed{F[x] \ / \ (p(x)) \text{ is a field}}$$

quadratics and cubics are reducible only if reduction contains linear factor.

only irreducible quartics:

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

characteristic of a field F is the smallest integer n such that

$$1^n = 1 + ... + 1 = 0$$

the characteristic of a field is either 0 or p.

All finite fields have order p^n for some prime p.

Exercises

1. Given an exmaple of a division ring that's not a field
   Quaternions $\mathbb{H}$, since $ij \neq ji$, hence not abelian;
   is a division ring since * inverses exist (complicated looking fraction)

2. What are the ideals of $\mathbb{Z}$?
   $n\mathbb{Z}$ for $n \in \mathbb{Z}$: $0, \mathbb{Z}, 2\mathbb{Z}$

3. What are the max ideals of $\mathbb{Z}$?
   n$\mathbb{Z}$ is maximal when $\mathbb{Z}/n\mathbb{Z}$ is a field, meaning n prime.

4. What the prime ideals of $\mathbb{Z}$? all of the above AND 0

Curiosities

Compose bijective functions bijection
This explains why composing cycles produces a cycle, aka a perumtation.
prove directly by thinking about steps of composition.

Open Questions

Open Questions

$$\boxed{\text{P is a prime ideal} \iff R/P \text{ is an integral domain}}$$

why?