1 Definition and examples of groups and subgroups

Definition 1.1 (Conjugacy class): Let G be a group. For $a, b \in G$, we say they are conjugates if there exists some $x \in G$ so that $xax^{-1} = b$. For $a \in G$, define the conjugacy class to be

$$cl(a) = cl_G(a) = \{b \in G \mid b \sim a\} = \{xax^{-1} \mid x \in G\}$$

Remark 1 Subgroup notation is $H \leq G$. □

Theorem 1.1 (Subgroup tests):

- Subgroup test 1: a subset H of G is a subgroup if and only if 1. contains identity, 2. closed under operation, 3. closed under inversion
- Subgroup test 2:a subset H of G is a subgroup if and only if 1. it is nonempty 2. for all $a, b \in H, ab^{-1} \in H$
- Finite subgroup test: G a group, H a finite subset of the group. Then $H \leq G$ iff 1. nonempty, 2. closed under operation.

Definition 1.2 (Dihedral group):

Definition 1.3 (Centre): Let G be a group. The center of it is the following subgroup.

$$Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$$

The centralizer of an element $a \in G$ is the following subgroup.

$$C_G(a) = \{x \in G \mid ax = xa\}$$

Center is the subgroup of elements that commutes with everything whereas centralizer (specific to an element) is all the elements that commutes with that particular element.

2 Cyclic groups and Generators

- Know what it's meant by: if G is a group, $S \subseteq G$, then subgroup of G generated by S means..
- Generators
- Finitely generated, cyclic

Remark 2 An interesting result Let G be a group and let $a \in G$. Then if $|a| = n$, we have $\langle a^k \rangle = \langle a^l \rangle$ iff $\gcd(n, k) = \gcd(n, l)$. The distinct subgroups of $\langle a \rangle$ are the subgroups of the form

$$\langle a^d \rangle = \{a^{kd} \mid k \in \mathbb{Z}_{n/d}\} = \{a^0, a^d, a^{2d}, \dots a^{n-d}\}$$

where $d \mid n$.
So if $a \in G$ with $|a| = n$, the order of a^k is a positive divisor of n, and for each positive divisor $d \mid n$, the number of elements in $\langle a \rangle$ of order d is $\phi(d)$. So for $n \in \mathbb{Z}^+$ we have $\sum_{d|n} \phi(d) = n$. □

Definition 2.1 (Free group): Have a set of S. $F(S)$ constructed by having words from S, works by concatenation and cancellation.

Definition 2.2 (Free abelian group): Abelianize free group. Characterized by the set of function that sends $S \to \mathbb{Z}$ with $f(a) = 0$ for all but finitely many $a \in S$.

3 Chapter 3. The symmetric group

Definition 3.1 (Array notation): Array notation for S_n.

For $n \geq 3$, we can think of D_n as a subgroup of S_n. As an element that permutes roots of unity.

Definition 3.2 (Cycle notation): $\alpha = (a_1, a_2, \ldots, a_\ell)$. As a theorem, every element in S_n can be written as a product of disjoint cycles.

Theorem 3.1:

- The order of a permutation: when a permutation is written in disjoint cycle notation, its order is the lcm of the lengths of the cycles.
- Conjugacy class of a Permutation: Let $\alpha, \beta \in S_n$. Then α, β are conjugates in S_n if and only if written in cycle notation, they have same number of cycles in each lenght.
- Even/odd permutations: every element in S_n is a product of $2-$cycles. If e can be written as a product of 2-cycles, then the number of 2-cycles that makes e is even. If an element a can be written as product of 2-cycles in two ways, then in both ways, the number of 2-cycles are consistent modulo 2.
- Parity is defined by number of 2-cycles in the 2-cycle notation.

Definition 3.3 (The alternating group A_n):
For $n \geq 2$, we define the alternating group A_n to be

$$A_n = \{\alpha \in S_n \mid (-1)^\alpha = 1\}$$

Note that $A_n \subseteq S_n$. Also $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$. We have a bijective correspondence between $A_n, S_n \setminus A_n$ by $F(\alpha) = (12)\alpha$.

4 Chapter 4. Homomorphisms and Isomorphisms of groups

Definition 4.1 (Endomorphism, automorphism): An endomorphism is a group homomorphism from a group G to itself. An automorphism is a group isomorphism to itself.

Theorem 4.1:
Let $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = 1$. Then

- $\mathbb{Z}_{ab} = \mathbb{Z}_a \times \mathbb{Z}_b$
- $U_{ab} = U_a \times U_b$

The U_k is the multiplicative group of elements rel.prime to k.

Definition 4.2 (Conjugation groups):
Given a group, then the map called conjugation by a, where $a \in G$ is given by

$$C_a(x) = axa^{-1}$$

Inner automorphism of G:

$$Inn(G) = \{C_a \mid a \in G\}$$

note that $Inn(G) \leq Aut(G)$.
Note that when $H \leq G$, we have

$$C_a(H) \cong H$$

The isomorphic groups H and $C_a(H) = aHa^{-1}$ are called conjugate subgroups of G.

Theorem 4.2 (Cayley's Theorem):
Let G be a group

- G is isomorphic to a subgroup of $perm(G)$. Consider the left multiplication L_a.
- If $|G| = n$ then G is isomorphic to a subgroup of S_n.

5 Chapter 5. Cosets, Normal subgroups, quotient groups

Definition 5.1 (Cosets):
Given a group G and a subgroup H, given $a \in H$, then left coset of H containing a is: aH.
The set of left cosets of H in G is:

$$G/H = \{aH \mid a \in G\}.$$

The index of G/H is $[G : H] = |G/H|$. Note this notation is also used in field extensions. We call these left cosets and right cosets. When G is abelian they are just cosets.

Theorem 5.1 (Properties of cosets):
Let $H \leq G, a \in G$. Then

- $b \in aH \iff a^{-1}b \in H \iff aH = bH$
- $|H| = |aH|$
- Either $aH = bH$ or $aH \cap bH = \varnothing$.

Corollary 5.2 (Lagrange's theorem):
$|G| = |G/H||H|$

Theorem 5.3 (Properties of normal subgroups):
Let $H \leq G$. Then TFAE

- The operation $* : G/H \times G/H$ by $(aH) * (bH) = (ab)H$ makes sense
- For any $a \in G$, $aHa^{-1} = H$
- For any $a \in G, aH = Ha$
- $aha^{-1} \in H, \forall h \in H, a \in G$

Definition 5.2 (Normal subgroups): When $H \leq G$ then H a normal subgroup of G, write $H \trianglelefteq G$. G/H is the quotient group of G by H.

Definition 5.3 (Simple groups): A group G is simple if $H \trianglelefteq G$ implies that $H = G$ or $H = \{e\}$.

Theorem 5.4 (The first isomorphism theorem):

1. if $\phi : G \to H$ is a homomorphism, then $K = ker(\phi) \trianglelefteq G$. Also $G/K \cong Im(\phi)$.

   The map
   $$\Phi : G/K \to Im(\phi), aK \to \phi(a)$$
   is the map that gives the desired isomorphism.
2. If $K \trianglelefteq G$, then the map $\phi : G \to G/K$ given by $\phi(a) = aK$ is the group homomorphism with $ker(\phi) = K$.

Theorem 5.5 (The second isomorphism theorem):
Let G be a group and $H \leq G$, $K \trianglelefteq G$. Then $K \cap H \trianglelefteq H, KH = \langle K \cup H \rangle$, and $H/(K \cap H) \cong KH/K$.

Theorem 5.6 (The third isomorphism theorem):
Let G be a group, let $H, K \trianglelefteq G$ with $K \leq H$. Then $H/K \trianglelefteq G/K$ and $(G/K)/(H/K) \cong G/H$.

Definition 5.4 (Centralizer, Normalizer): Let $H \leq G$. Then centralizer of H is:

$$C(H) = \{a \in G \mid ah = ha, \forall h \in H\}$$

Let $H \leq G$. Then normalizer of H is:

$$N(H) = \{a \in G \mid aH = Ha\}$$

Theorem 5.7 (The normalizer/centralizer theorem):
Let $H \leq G$, then $C(H) \trianglelefteq N(H)$ and $N(H)/C(H)$ is isomorphic to a subgroup of $Aut(H)$.

Theorem 5.8 (Characterization of internal direct products):
Let G be a group. Let $H \trianglelefteq G, K \trianglelefteq G$. Suppose $H \cap G = \{e\}$ and $G = HK$. Then $G \cong H \times K$

Theorem 5.9 (simple A_n):
for $n \geq 5$, A_n is simple.

6 Chapter 6. Group actions on sets

Definition 6.1 (Representation):
Let G be a group. A representation of a G is a group homomorphism $\phi : G \to perm(S)$ for some set S. A representation is called faithful when it is injective.

Definition 6.2 (Group action):
Let G be a group, let S be a set. A group action of G on S is a map from $G \times S \to S$ such that $e \cdot x = x, (ab)x = a(bx), \forall x \in S, a, b \in G$. A group action is faithful if its corresponding representation is also faithful.

Definition 6.3 (Fixed set, orbit, stabilizer):
Let G be a group which acts on a set S. Let $a \in G$.
The fixed set of a is

$$Fix(a) = \{x \in S \mid ax = x\} \subseteq S$$

The orbit of an element $x \in S$ is

$$Orb(x) = Gx = \{ax \mid a \in G\} \subseteq S$$

Note that elements in one another's orbits is an equivalence relation. So the notation S/G makes sense.

The stablizer of an element $x \in S$ is

$$Stab(x) = \{a \in G \mid ax = x\} \leq G$$

Theorem 6.1 (Orbit-stabilizer theorem):
Let G be a group acting on a set S. Then for $x \in S$, we have

$$|G| = |Orb(x)||Stab(x)|$$

Definition 6.4 (Class equation):

$$|G| = \sum |G/C(x_i)|$$

Definition 6.5 (Cauchy's theorem): G is a finite group. Let p be a prime divisor of $|G|$. Then G contains an element of order p. Indeed

$$|\{a \in G \mid |a| = p\}| = p - 1 \pmod{(p-1)p}$$

Theorem 6.2:
G a finite group, $H \leq G$. Suppose $|G/H| = p$. where p is the smallest prime divisor of $|G|$. Then H is a normal subgroup of G.

Theorem 6.3 (Burnside lemma):
Good for counting vertex coloring.

7 Chapter 7. The classification of Finite abelian groups

Definition 7.1 (Free abelian group): groups isomorphic to $\mathbb{Z}^n$.

Theorem 7.1 (Subgroups and quotient groups of $\mathbb{Z}^n$):
Let G be a free abelian group of rank n. Let $H \leq G$. Then H is a free abelian group of rank r for some $0 \leq r \leq d$ and

$$H \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

with $d_1 \mid d_2, d_2 \mid d_3, \ldots, d_{r-1} \mid d_r$.

Theorem 7.2:
very finite abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_l}$$

for some integer $\ell \geq 0$ and some integers n_i with $2 \leq n_1, n_1 \mid n_2, n_2 \mid n_3, \ldots, n_{l-1} \mid n_l$.
Alternatively, every finite abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}$$

such that whenever $p_1 \leq p_2 \leq \ldots \leq p_m$. If $p_i = p_{i+1}$ then must have $k_i \leq k_{i+1}$. All the k_is are positive integers.

Corollary 7.3 (Classification of Finite Abelian groups):
Let G, H be finite abelian groups. If G, H have same number of elements of each order, then $G \cong H$.

Corollary 7.4 (number of distinct abelian groups):
Let $n = \prod p_i^{k_i}$, distinct notation. Then number of distinct abelian groups of order N is equal to $\prod P(k_i)$ where K is the number of partitions.

8 Chapter 8. Definitions and examples of rings and subrings.

Definition of rings: a set R with two binary operations, addition denoted by $+$, multiplication by $\times$, and 0-additive identity. With the following properties:

- $+$ is associative
- $+$ is commutative
- 0 is additive identity
- Everything has a inverse under $+$
- $\times$ is associative
- $\times$ distributive over $+$

Basically, it's an abelian group under $+$ with additional properties: $\times$ is associative and distributive.

- commutative ring
- ring has identity
- a ring element is invertible (if it has a 1)
- division ring: a ring where every element is invertible
- field: commutative division ring
- units in ring: (if R has a 1, and $a \in R$ has multiplicative inverse, then a is a unit of R.)
- left inverse

- right inverse
- zero divisors
- integral domain
- characteristic of a ring
- Center of a ring is a subring

Theorem 8.1:

- R is a finite ring. It is a field if and only if it's an ID.
- Let R be a ring with 1 and no zero divisors. THen either $char(R) = 0$ or $char(R)$ is prime.
- Subring tests and subfield tests
-

9 Chapter 9 Ring Homomorphisms, Ideals, quotient rings

Definition 9.1:

- ring homomorphism ($+, \times$ structures preserved)
- ideals
- generated ideals by a subset
- finitely generated ideal
- principle ideal

Theorem 9.1:

- Intersection, sum, and products of ideals are ideals
- Given a set $U \subseteq R$, how to generate the ideal corresponding to that set.

Theorem 9.2 (First isomorphism theorem):
Let $\phi : R \to S$ be a homomorphism of rings. $K = ker(\phi)$. Then K is an ideal of R and

$$R/K \cong \phi(R)$$

Theorem 9.3 (Second isomorphism theorem):
A, B are ideals in R. Then A is an ideal of $A + B$ and $A \cap B$ is an ideal in B.

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

Theorem 9.4 (Third isomorphism theorem):
A, B are ideals in R with $A \subseteq B \subseteq R$. Then B/A is an ideal fo R/A and

$$(R/A)/(B/A) \cong R/B$$

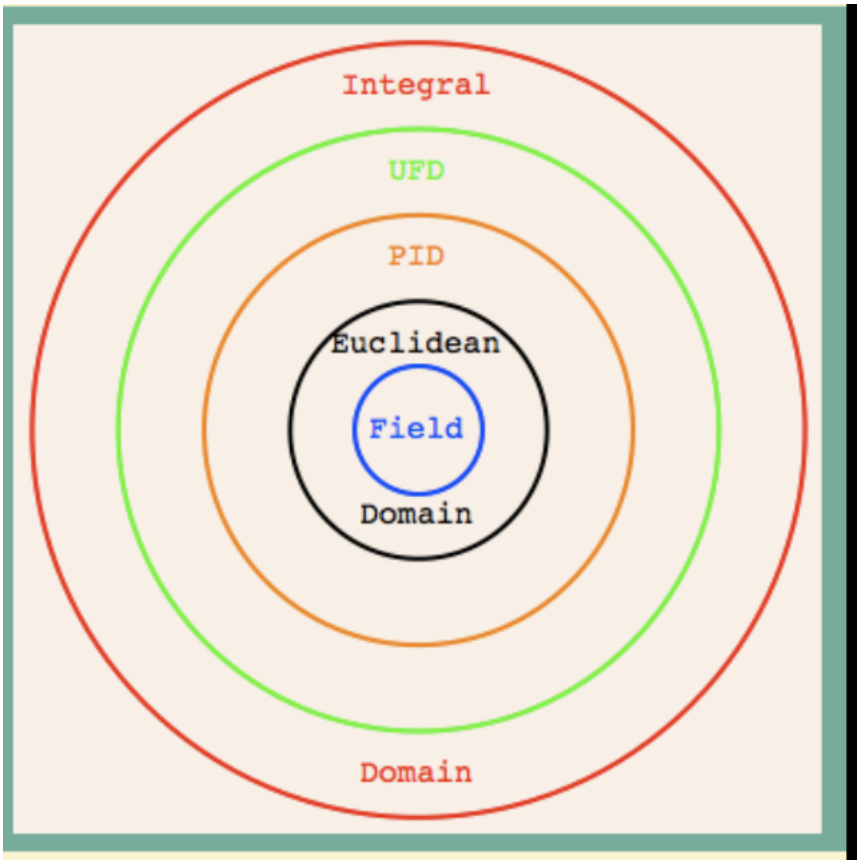
10 Chapter 10. Factorization in commutative rings

Definition 10.1:

- Prime ideal
- maximal ideal
- Divisors and associates in commutative rings
- ring elements that are reducible, irreducible, prime
- Euclidean domain
- Principal ideal domain
- Unique factorization domain
- Noetherian ring

Theorem 10.1:

- An ideal is prime if and only if...
- Let R be a commutative ring with 1. Let P be an ideal in R. Then P is prime if and only if R/P is an integral domain.
- Let R be a commutative ring with 1. Show that every maximal ideal in R is also prime.
- Let R be a commutative ring with 1. Let M be an ideal in R. Then M is maximal if and only if R/M is a field.
- Associates have the same properties in being reducible, irreducible, unit, prime.


Integral
UFD
PID
Euclidean
Field
Domain
Domain