Abstract Algebra Summary Sheet

By Danny Liu

1 Groups

A group is a nonempty set G together with a binary operator $\cdot$ such that the following hold
(1) Closure: For all $a, b \in G$, $ab \in G$
(2) Associativity: For all $a, b, c \in G$, $(ab)c = a(bc)$
(3) Identity: There exists $e \in G$ such that for all $a \in G$, $ae = a = ea$
(4) Inverse: For all $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = e$

The order of an element is the smallest number n such that $a^n = e$
A group is Abelian (commutative) if $ab = ba$ for all $a, b \in G$
The inverse and identity are unique.
A subgroup of a group G is a subset H that is also a group under the operation of G.
$\{e\}$ is the trivial subgroup and a proper subgroup of G is a subgroup of G that is not equal to G.
Some common groups are $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}^*, \cdot \rangle$, $\langle \mathbb{Z}_p^*, \cdot \rangle$, $\mathbb{Z}_n$, $U(n)$, $GL(n, F)$ and D_n

1.1 Subgroup Test

Let G be a group and H a nonempty subset of G. Then $H \leq G$ if
(1) $a, b \in H \implies ab \in H$ (closure)
(2) $a \in H \implies a^{-1} \in H$ (inverse)

2 Cyclic Groups

Define $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ as the cyclic subgroup of G generated by $a \in G$
Define $Z(G) = \{a \in G \mid ab = ba \text{ for all } b \in G\}$ as the center of G
Define $C(a) = \{b \in G \mid ab = ba\}$ as the centralizer of a in G
If there exists $a \in G$ such that $G = \langle a \rangle$, then G is cyclic.
Every cyclic group is Abelian. Center of an Abelian group is the group itself.

2.1 Criterion for $a^i = a^j$

Let G be a group and $a \in G$. If $|a| = \infty$, then $a^i = a^j$ if and only if $i = j$
If $|a| = n$, then $\langle a \rangle = \{e, a^1, a^2, ..., a^{n-1}\}$ and $a^i = a^j$ if and only if $n | i - j$

2.2 Criterion for $\langle a^i \rangle = \langle a^j \rangle$

Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $gcd(n, i) = gcd(n, j)$. Moreover, $|a^i| = {}^{n}/_{gcd(n,\, i)}$.

2.2.1 $\mathbb{Z}_n$ generators

An integer $k \in \mathbb{Z}_n$ is a generator for $\mathbb{Z}_n$ if and only if $n \perp k$.

2.3 Fundamental Theorem of Cyclic Groups

(1) Every subgroup of a cyclic group is cyclic.
(2) If $k|n$, then $\langle a \rangle$ has only one subgroup of order k, namely $\langle a^{n/k} \rangle$

2.4 Number of Elements of Order d

If $d|n$, then the number of elements of order d in a cyclic group of order n is $\phi(d)$
In a finite group, the number of elements of order d is divisible by $\phi(d)$

3 Permutation Groups

A permutation on a set A is a bijective function from A to A.
A permutation group of a set A is a set of permutations of A that forms a group under function composition. Since elements are irrelevant, denote $A = \{1, 2, ..., n\}$
$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$ can be written in cycle notation as $\alpha = (12)(346)(5)$
An expression of the form $(a_1, a_2, ..., a_m)$ is an m-cycle.
A transposition is a cycle of length 2.
The set of all permutations of A is called the symmetric group of degree n, denoted S_n

3.1 Disjoint Cycles

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.
If a pair of cycles α and β have no entries in common, then $\alpha\beta = \beta\alpha$
The order of a permutation of a finite set written in disjoint cycles is the lcm of the lengths of the cycles. (Think α^n is the identity permutation.)

3.2 Multiplying Cycles

Composition is right to left and we write down one number after finishing the composition chain once. Close cycle if the end of a composition chain is what we started with, else repeat.
Verify that $(1523)(46)(13)(456) = (2354)$, $(1234) = (14)(13)(12)$, and $(12)^{-1} = (12)$

3.3 Product of Transpositions

Every permutation in S_n with $n > 1$ is a product of 2-cycles (transpositions).
If a permutation α can be expressed as a product of an even number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even number of 2-cycles.
A permutation is even if it can can be expressed as an even number of 2-cycles.
The identity is an even permutation.
$A_n = \{\alpha \in S_n \mid \alpha \text{ is even}\}$ is the alternating group of S_n.

4 Isomorphisms

An isomorphism is a bijective function from a group G to a group $\bar{G}$ that preserves the group operation. Isomorphic groups share all group-theoretic properties in common.
An automorphism is an isomorphism from a group to itself.
$\phi_a(x) = axa^{-1}$ is the inner automorphism of G induced by a.
$Inn(G) = \{\phi_a \mid a \in G\}$ is the group of all inner automorphisms of G.

For any positive integer n, $Aut(\mathbb{Z}_n) \cong U(n)$ where $Aut(G)$ is the set of all automorphisms of G.
A group of order $2p$ is isomorphic to either $\mathbb{Z}_{2p}$ or D_p where p is an odd prime.

4.1 Cayley's Theorem

Let $\bar{G} = \{T_g \mid g \in G\}$ where $T_g(x) = gx \ \forall x \in G$ be the left regular representation of a group G. Then every group G is isomorphic to the permutation group $\bar{G}$.

5 Cosets and Legrange's Theorem

Let $H \leq G$. Then the left-coset of H in G containing $a \in G$ is $aH = \{ah \mid h \in H\}$

5.1 Coset Properties

Let $H \leq G$ and $a, b \in G$, then
(1) $a \in aH$
(2) $aH = H$ if and only if $a \in H$
(3) $(ab)H = a(bH)$
(4) $aH = bH$ if and only if $a^{-1}b \in H$
(5) $aH = bH$ or $aH \cap bH = \emptyset$
(6) $|aH| = |bH|$
(7) $aH = Ha$ if and only if $H = aHa^{-1}$
(8) $aH \leq G$ if and only if $a \in H$
Notice that properties 1, 5 and 6 imply the left cosets of a subgroup $H \leq G$ partition G into blocks of equal size. These are the equivalence classes under the relation $a \sim b$ if and only if $aH = bH$

5.2 Legrange's Theorem

In a finite group, the order of a subgroup divides the order of the group.
In a finite group, the order of each element of the group divides the order of the group.
A group of prime order is cyclic.
The number of distinct left and right cosets of H in G, denoted $[G : H] = {}^{|G|}/_{|H|}$

5.3 Orbit Stabilizer Theorem

Let G be a permutation group on a set S. Define the stabilizer of $i \in S$ in G as the set of permutations in G that leave i unchanged and the orbit of i under G as the set of elements of in S that get generated by applying every permutation in G to i. Then $|G| = |\text{orb}_G(i)||\text{stab}_G(i)|$

6 External Direct Products

The order of an element in a direct product of a finite number of finite groups is the lcm of the orders of the components of the element.
Let G and H be finite cyclic groups. Then $G \bigoplus H$ is cyclic if and only if $|G| \perp |H|$
Let $m = n_1 n_2 ... n_k$. Then $\mathbb{Z}_m = \mathbb{Z}_{n_1} \bigoplus \mathbb{Z}_{n_2} \bigoplus ... \bigoplus \mathbb{Z}_{n_k}$ if and only if $n_i \perp n_j$ whenever $i \neq j$.
Define $U_k(n) = \{x \in U(n) \mid x \equiv_k 1\}$. Then $U_k(n) \leq U(n)$ and $U_s(st) \cong U(t)$ whenever $s \perp j$.
Let $m = n_1 n_2 ... n_k$ and $n_i \perp n_j$ whenever $i \neq j$, then $U(m) \cong U(n_1) \bigoplus U(n_2) \bigoplus ... \bigoplus U(n_k)$.
$U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}}$ for any odd prime and integer n.

7 Normal Subgroups

A subgroup H of G is normal in G if $aH = Ha$ for all $a \in G$
When a subgroup is normal, the set of left cosets of H in G is called the factor group of G by H

7.1 Normal Subgroup Test

$H \triangleleft G$ if and only if $gHg^{-1} \subseteq H$ for all $g \in G$

7.2 Factor Groups

Let $H \triangleleft G$, then $G/H = \{aH \mid a \in G\}$ is a group under the group operation $(aH)(bH) = abH$
Let $Z(G)$ be the center of some group G. If $G/Z(G)$ is cyclic, then G is Abelian
For any group G, $G/Z(G) \cong \text{Inn}(G)$

7.3 Cauchy's Theorem

Let G be a finite Abelian group and p be a prime that divides the order of G, then G has an element of order p.

8 Homomorphisms

A homomorphism is a mapping that preserves the group operation.
Every linear transformation is a group homomorphism; an invertible linear transformation is a group isomorphism.
If $\phi : G \to \bar{G}$ is a homomorphism, then $\phi(G) = \{\phi(x) \mid x \in G\}$ is the homomorphic image of G
$\phi(G) = \bar{G}$ if and only if ϕ is onto
Ker $\phi = \{x \in G \mid \phi(x) = e\}$ is the set of all elements in G that map to the identity in $\bar{G}$

8.1 Homomorphism Properties

Let ϕ be a homomorphism from G to $\bar{G}$, $g \in G$ and $H \leq G$, then
(1) $\phi(e) = \bar{e}$
(2) $\phi(g^n) = [\phi(g)]^n$
(3) If $|g|$ is finite, then $|\phi(g)| \mid |g|$
(4) Ker $\phi \leq G$
(5) $\phi(a) = \phi(b)$ if and only if $a\text{Ker}\phi = b\text{Ker}\phi$
(6) If $\phi(g) = \bar{g}$, then $\phi^{-1}(\bar{g}) = \{x \in G \mid \phi(x) = \bar{g}\} = g\text{Ker}\phi$
(7) $\phi(H) = \{\phi(h) \mid h \in H\} \leq \bar{G}$
(8) If H is cyclic or Abelian, then so is $\phi(H)$
(9) If H is normal in G, then so is $\phi(H)$ in $\phi(G)$
(10) $|\text{Ker } \phi| = n$ implies ϕ is an $n-1$ mapping
(11) $\bar{K} \leq \bar{G}$ implies $\phi^{-1}(\bar{K}) = \{k \in G \mid \phi(k) \in \bar{K}\} \leq G$
(12) $\bar{K} \triangleleft \bar{G}$ implies $\phi^{-1}(\bar{K}) \triangleleft G$
(13) If ϕ is onto and Ker $\phi = \{e\}$, then ϕ is an isomorphism.

8.2 First Isomorphism Theorem

Let $\phi : G \to \bar{G}$ be a homomorphism, then $G/\text{Ker } \phi \cong \phi(G)$

8.2.1 Corollary

If ϕ be a homomorphism from a finite group G to $\bar{G}$, then $|\phi(G)|$ divides $|G|$ and $|\bar{G}|$

8.3 Normal Subgroups are Kernels

Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N

9 Finite Abelian Groups

9.1 Fundamental Theorem of Finite Abelian Groups

Every finite Abelian group is a direct product of cyclic groups of prime power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group. (These direct products form isomorphism classes)

9.1.1 Corollary

If m divides the order of a finite Abelian group G, then G has a subgroup of order m.

10 Rings

A ring R is a nonempty set with two binary operations, addition $(+)$ and multiplication $(\cdot)$ such that R is an additive Abelian group and is associative and distributive with multiplication.
If multiplication in R is commutative, then R is a commutative ring.
If R has a nonzero multiplicative identity, then R is a ring with unity.
$a \in R$ is a unit if its multiplicative inverse $a^{-1} \in R$ exists.
If a ring has a unity it is unique and likewise for any ring element's multiplicative inverse.

10.1 Direct Sums

Let $R_1 ... R_n$ be rings, then $R_1 \bigoplus ... \bigoplus R_n$ is a ring with $(+)$ and $(\cdot)$ defined component-wise.
$R_1 \bigoplus ... \bigoplus R_n = \{(a_1, ..., a_n) \mid a_i \in R_i\}$

10.2 Subring Test

A subring S of a ring R is a subset of R which is itself a ring under the operations of R.
A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication. That is, for all $a, b \in S$, $a - b \in S$ and $ab \in S$

11 Integral Domains

A zero-divisor of a commutative ring R is a nonzero element $a \in R$ s.t $\exists b \in R$, $b \neq 0$ with $ab = 0$
An integral domain is a commutative ring with unity and no zero-divisors, i.e $ab = 0$ implies $a = 0$ or $b = 0$. Also defined as commutative rings with unity in which cancellation property holds.

11.1 Fields

A field is a commutative ring with unity in which every nonzero element is a unit. Also defined as a ring in which the nonzero elements form an Abelian group under multiplication.
Every field is an integral domain but only finite integral domains are fields.
For every prime p, Z_p is a field.

11.2 Classic Examples

$\mathbb{Z}$ and $\mathbb{Z}_n$ are commutative rings with unity; $2\mathbb{Z}$ is a commutative ring.
$\mathbb{Z}$ is an integral domain; $\mathbb{R}$ and $\mathbb{Q}$ are fields.

12 Ideals

A subring A of R is an ideal of R if $ar \in A$ and $ra \in A$ for all $r \in R$, $a \in A$
Ideals absorb all elements of R, $rA \subseteq A$ and $Ar \subseteq A$ for all $r \in R$
$\{0\}$ is the trivial ideal and R is always an ideal by closure.
$\langle a \rangle = \{ra \mid r \in R\}$ is the principal ideal of R generated by a.
A prime ideal A of a comm ring R is a proper ideal s.t for all $a, b \in R$, $ab \in A$ implies $a \in A$ or $b \in A$
A maximal ideal A of a comm ring R is a proper ideal s.t whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$. Maximal ideals are prime ideals.

12.1 Ideal Test

A nonempty subset A of a ring R is an ideal of R if (1) $a - b \in A$ for all $a, b \in A$ and
(2) $ra \in A$, $ar \in A$ for all $a \in A$, $r \in R$

12.2 Factor Rings

Let R be a ring, A a subring of R. Then the ${}^{R}\!/_{A} = \{r + A \mid r \in R\}$ is a ring under the operations $(a + A) + (b + A) = (a + b) + A$ and $(a + A)(b + A) = ab + A$ if and only if A is an ideal of R.

12.2.1 ${}^{R}\!/_{A}$ as Integral Domain and Field

Let R be a commutative ring with unity and A an ideal of R. Then
(1) ${}^{R}\!/_{A}$ is an integral domain if and only if A is prime.
(2) ${}^{R}\!/_{A}$ is a field if and only if A is maximal.

13 Ring Homomorphisms

Same as group homomorphisms, but now also preserve multiplication.

13.1 Kernels are Ideals

Let ϕ be a ring homomorphism from R to S. Then Ker $\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

13.2 First Ring Isomorphism Theorem

Let ϕ be a ring homomorphism from R to S, then ${}^{R}\!/_{\text{Ker } \phi} \cong \phi(R)$

13.3 Ideals are Kernels

Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \to r + A$ from R to R/A

13.4 Field of Quotients

Let D be an integral domain, then there exists a field F that contains a subring isomorphic to D.

14 Miscellaneous

14.1 Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ with $0 \leq r < b$

14.2 Bezout's Identity

For any nonzero integers a and b, there exist integers s and t such that $gcd(a, b) = as + bt$. Moreover $gcd(a, b)$ is the smallest integer of the form $as + bt$

14.2.1 Bezout's Lemma

If $a \perp b$, then there exist integers s and t such that $as + bt = 1$

14.3 Euler's Lemma

If p is prime and $p|ab$, then either $p|a$ or $p|b$

14.4 Fermat's Little Theorem

For every integer a and prime p, $a^{p-1} \equiv_p 1$

14.5 Equivalence Relations

A binary relation $\sim$ on a set X is an equivalence relation on X if and only if
(1) $a \sim a$ for all $a \in X$ (reflexive)
(2) $a \sim b \implies b \sim a$ for all $a, b \in X$ (symmetric)
(3) $a \sim b$ and $b \sim c \implies a \sim c$ for all $a, b, \in X$ (transitive)

$[a] = \{x \in X \mid x \sim a\}$ is the equivalence class of X containing a.
The equivalence classes of an equivalence relation on a set X constitute a partition of X. Conversely, for any partition P of X, there is an equivalence relation on X whose equivalence classes are the elements of P.

14.6 Functions

A function is bijective if and only if it is invertible.
Function composition is associative and preserve injectivity (one-to-one) and surjectivity (onto).