Math 280 Quick Reference

Groups

Closed — An operation $*$ is closed on a set S if $s * t$ is in S for all $s, t \in S$

Group — A set G together with a closed binary operation $*$ such that

1. G contains an identity e: $e * g = g * e = g$ for all $g \in G$
2. Every $g \in G$ has an inverse g^{-1}: $g * g^{-1} = g^{-1} * g = e$
3. $*$ is associative: $g * (h * j) = (g * h) * j$ for all $g, h, j \in G$

Order (of Group), $|G|$ — The number of elements in the group

Finite Group — A group with finite order

Order (of Element), $|g|$ — The smallest positive integer n such that

- $g^n = e$ in a multiplicative group
- $ng = e$ in an additive group

Trivial Group — The group containing a single element (the identity)

Abelian — A commutative group: $g * h = h * g$ for all $g, h \in G$

Cyclic — A group generated by a single element, g; that is, all elements in the group can be written as

- a power of g in a multiplicative group
- a multiple of g in an additive group

Generator — An element that generates a cyclic group

Subgroup — H is a subgroup of G if

1. H is a subset of G
2. H forms a group under the same operation as G

Generated Subgroup, $\langle g \rangle$ — The subgroup containing all elements of the form

- g^i in a multiplicative group
- ig in an additive group

Center, $Z(G)$ — The largest possible commutative subgroup of G. Equal to G if G is Abelian.

Centralizer, $C(g)$ — The subgroup of G containing all elements that commute with the (fixed) element g

Direct Product, $G \times H$ — The group of all tuples (g, h) for $g \in G, h \in H$.

Group Morphisms

Function	A map $f : X \to Y$ such that for all $x \in X$, if $f(x) = y_1$ and $f(x) = y_2$, then $y_1 = y_2$
Surjection	A map $f : X \to Y$ such that for all $y \in Y$, there exists some $x \in X$ with $f(x) = y$
Injection	A map $f : X \to Y$ such that if $f(x_1) = f(x_2)$, then $x_1 = x_2$ for all $x_1, x_2 \in X$
Bijection	A map that is both injective and surjective
Group Homomorphism	A map $\phi : G \to H$ from a group G to a group H that preserves operations: $$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$$ May not be surjective nor injective
Group Isomorphism	A bijective group homomorphism
Isomorphic Groups	Two groups with an isomorphism between them; considered equivalent algebraic structures
Kernel, ker(ϕ)	The subgroup of G mapped to the identity in H. Trivial if ϕ is an isomorphism
Group Automorphism	An isomorphism from a group to itself, $\phi : G \to G$

Permutations

Disjoint Cycle Notation	A method of expressing a permutation as a product of cycles that do not repeat letters, ie $(1\ 3)(2\ 4)$
Length of a Cycle	The number of letters in a cycle
Transposition	A cycle with length 2
Fixed Point	A letter that is unchanged by the permutation, will appear in a cycle with length 1
Even Permutation	A permutation that can be written as a product of an even number of (not necessarily disjoint) transpositions
Sign	The parity of a permutation, either even or odd, sometimes written +1 or -1 respectively
Order	The order of the permutation in S_n, equal to the least common multiple of its disjoint cycle lengths
Inverse	Found by "reversing" all cycles, ie $(1\ 3\ 4\ 2)^{-1} = (1\ 2\ 4\ 3)$

Rings

Ring — A set R together with additive and multiplicative operations $+, \cdot$ such that
1. R forms an Abelian group under $+$
2. $\cdot$ is associative: $r \cdot (s \cdot t) = (r \cdot s) \cdot t$ for all $r, s, t \in R$
3. $\cdot$ distributes over $+$: $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$ for all $r, s, t \in R$

Ring with Unity — A ring that contains a multiplicative identity

Commutative Ring — A ring with a commutative multiplicative operation

Unit — An element of a ring that has a multiplicative inverse in the ring

Subring — S is a subring of R if
1. S is a subset of R
2. S forms a ring under the same operations as R

Ideal — A subring I of a ring R such that $r \cdot a$ and $a \cdot r$ are in I for all $r \in R$, $a \in I$

Principal Ideal, $\langle a \rangle$ — An ideal of a ring R generated by a:

$$\langle a \rangle = \{ra \ : \ r \in R\}$$

Zero Divisor — r is a zero divisor in a ring R if there is some $s \in R$ with $r \cdot s = 0$.

Integral Domain — A ring with no zero divisors

Field — A commutative ring with unity in which every nonzero element is a unit (as close as possible to forming a group under addition and multiplication)

Characteristic of a Ring — The smallest positive integer n with $n \cdot r = 0$ for all r in the ring, or 0 if no such integer exists

Ring Morphisms

Ring Homomorphism — A map $\phi : R \to S$ from a ring R to a ring S that preserves both operations:

$$\phi(r_1 \cdot_R r_2) = \phi(r_1) \cdot_S \phi(r_2)$$

$$\phi(r_1 +_R r_2) = \phi(r_1) +_S \phi(r_2)$$

Ring Isomorphism — A bijective ring homomorphism

Useful Theorems

Shoes & Socks Principle For g, h in a group G, $(gh)^{-1} = h^{-1}g^{-1}$

Two Step Subgroup Test H is a subgroup of G if

1. $ab \in H$ for all $a, b \in H$ (H is closed)
2. $a^{-1} \in H$ for all $a \in H$

One Step Subgroup Test H is a subgroup of G if $ab^{-1} \in H$ for all $a, b \in H$

Lagrange's Theorem The order of a subgroup divides the order of the group

Fundamental Theorem of Cyclic Groups Every subgroup of a cyclic group is cyclic. Moreover, if G is a cyclic group of order n and k divides n, there is exactly one subgroup of G with order k.

Group Isomorphism Properties If $\phi : G \to H$ is a group isomorphism then

- $\phi(e_G) = e_H$
- G, H have the same order
- If G, H are finite, they have the same number of elements of order k
- $\phi(g^n) = \phi(g)^n$ for all $g \in G$
- $|g| = |\phi(g)|$
- G is Abelian iff H is Abelian
- G is cyclic iff H is cyclic
- ϕ is invertible and $\phi^{-1} : H \to G$ is an isomorphism
- If K is a subgroup of G then $\phi(K)$ is a subgroup of H
- If $Z(G)$ is the center of G then $\phi(Z(G))$ is the center of H

Isomorphisms of Cyclic Groups Every finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$, and every infinite cyclic group is isomorphic to $\mathbb{Z}$

Injective Test A homomorphism is injective if and only if its kernel is trivial

Cayley's Theorem Every group is isomorphic to some group of permutations

Corollary of Lagrange Every group of prime order is cyclic

Fundamental Theorem of Arithmetic Every integer $x > 1$ can be written as a product of prime numbers, unique up to commutativity

Fundamental Theorem of Algebra Every degree n single variable polynomial with complex coefficients has exactly n complex roots

Fundamental Theorem of Finite Abelian Groups Every finite Abelian group can be written as a direct product of cyclic groups of prime power order

Cancellation Law If a, b, c are elements of an integral domain with $a \neq 0$ and $ab = ac$, then $a = c$

Finite Field Test Every finite integral domain is a field

Important Groups

Name	Description	Order	Operation	Abelian†	Cyclic†
$\{e\}$	Trivial group	1	Add or Mult	Yes	Yes
$\mathbb{Z}$	Integers	∞	Real Add	Yes	Yes
$\mathbb{Z}_n$	Integers mod n, $\{0, 1, 2, \ldots, n-1\}$	n	Add mod n	Yes	Yes
$n\mathbb{Z}$	Integers that are multiples of n	∞	Add	Yes	Yes
$U(n)$	Multiplicative group of integers modulo n; positive integers less than and relatively prime to n	$\phi(n)$††	Mult mod n	Yes	No
$\mathbb{R}$	Real Numbers	∞	Real Add	Yes	No
$\mathbb{R}^*$	Nonzero real numbers	∞	Real Mult	Yes	No
$\mathbb{Q}$	Rational Numbers	∞	Real Add	Yes	No
$\mathbb{Q}^*$	Nonzero rational numbers	∞	Real Mult	Yes	No
$\mathbb{C}$	Complex Numbers	∞	Complex Add	Yes	No
$\mathbb{C}^*$	Nonzero complex numbers	∞	Complex Mult	Yes	No
$M_{n\times m}(\mathbb{R})$	$n \times m$ matrices with real entries	∞	Matrix Add	Yes	No
$GL_n(\mathbb{R})$	General linear group of $n \times n$ invertible matrices with real entries	∞	Matrix Mult	No	No
$SL_n(\mathbb{R})$	Special linear group of $n \times n$ invertible matrices with real entries and determinant 1	∞	Matrix Mult	No	No
$O_n(\mathbb{R})$	Orthogonal group of $n \times n$ matrices Q such that $Q^TQ = QQ^T = I$	∞	Matrix Mult	No	No
S_n	Symmetric group of all permutations on n letters	$n!$	Perm Mult	No	No
A_n	Alternating group of even permutations on n letters	$\frac{n!}{2}$	Perm Mult	No	No
D_n	Dihedral group of symmetries of a regular convex n-gon	$2n$	Composition	No	No
$\mathbb{Z}[i]$	Gaussian integers; all complex numbers of the form $a + bi$ with $a, b \in \mathbb{Z}$	∞	Complex Add	No	No

†: Reflects whether property can be assumed in general. Symmetric groups can be Abelian, for instance, but in general they are not.

††: Euler's totient function, number of positive integers x less than and relatively prime to n.

Important Rings

Name	Description	Characteristic	Commutative†	Unity	Zero Divisors†	Integral Domain	Field
$\{0\}$	Zero ring (aka trivial ring)	1	Yes	Yes	No	No	No
$\mathbb{Z}$	Integers	0	Yes	Yes	No	Yes	No
$n\mathbb{Z}$	Integers that are multiples of n	0	Yes	Yes	No	Yes	No
$\mathbb{Q}$	Rational numbers	0	Yes	Yes	No	Yes	Yes
$\mathbb{R}$	Real numbers	0	Yes	Yes	No	Yes	Yes
$\mathbb{C}$	Complex numbers	0	Yes	Yes	No	Yes	Yes
$\mathbb{Z}_n$	Integers mod n, $\{0, 1, 2, \ldots, n-1\}$, where n is not prime	n	Yes	Yes	Yes	No	No
$\mathbb{Z}_p$	p-adic integers; Integers mod p where p is prime	p	Yes	Yes	No	Yes	Yes
$M_{n\times n}(\mathbb{R})$	All $n \times n$ matrices with real entries	0	No	Yes	Yes	No	No
$\mathbb{Z}[x]$	Polynomials in indeterminate x with integer coefficients	0	Yes	Yes	No	Yes	No
$\mathbb{R}[x]$	Polynomials in indeterminate x with real coefficients	0	Yes	Yes	No	Yes	No
$\mathbb{Z}[i]$	Gaussian integers; all complex numbers of the form $a + bi$ with $a, b \in \mathbb{Z}$	0	Yes	Yes	No	Yes	No
$\mathcal{C}[x]$	Continuous real valued functions defined on $\mathbb{R}$	0	Yes	Yes	No	No	No

†: Reflects whether property can be assumed in general. Matrix rings can be commutative, for instance, but in general they are not.