MATH 4389–ALGEBRA 'CHEATSHEET'–BLECHER

- All numbers below are integers, usually positive.
- Read up on e.g. wikipedia on the Euclidean algorithm.
- Diophantine equation $ax + by = c$ has solutions iff $\gcd(a, b)$ doesn't divide c. One may find the solutions using the Euclidean algorithm (google this).
- Euclid's lemma: prime $p|ab$ implies $p|a$ or $p|b$.
- $\gcd(m, n) \cdot \text{lcm}(m, n) = mn$.
- $a \equiv b \pmod{m}$ means $m|(a - b)$. An equivalence relation (reflexive, symmetric, transitive) on the integers.
- $ax \equiv b \pmod{m}$ has a solution iff $\gcd(m, a)|b$.
- Division Algorithm: there exist unique integers q and r with $a = bq + r$ and $0 \leq r < b$; so $a \equiv r \pmod{b}$.
- Fermat's theorem: If p is prime then $a^p \equiv a \pmod{p}$ Also, $a^{p-1} \equiv 1 \pmod{p}$ if p does not divide a. (Little Fermat)
- For definitions for groups, rings, fields, subgroups, order of element, etc see Algebra fact sheet" below.
- $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$ with addition and multiplication mod m, is a group and commutative ring $(= \mathbb{Z}/m\mathbb{Z})$
- Order of n in $\mathbb{Z}_m$ (i.e. smallest k s.t. $kn \equiv 0 \pmod{m}$) is $m/\gcd(m, n)$.
- $\langle a \rangle$ denotes the subgroup generated by a (the smallest subgroup containing a). For example $\langle 2 \rangle = \{0, 2, 2+2 = 4, 2+2+2 = 6\}$ in $\mathbb{Z}_8$. (In ring theory it may be the subring generated by a).
- A cyclic group is a group that can be generated by a single element (the group generator). They are abelian.
- A finite group is cyclic iff $G = \{g, g+g, \cdots, g+g+\cdots+g = 0\}$; so $G = \langle g \rangle$. The only infinite cyclic group is $\mathbb{Z}$ (up to group isomorphism).
- If a has order n then $\langle a \rangle$ is isomorphic to the cyclic group of order n
- Any two cyclic groups of the same order are isomorphic.
- Any group of prime order is cyclic.
- Cauchy theorem: if a prime p divides $|G|$ there exist elements, hence subgroups, of order p
- Lagrange theorem (see "Algebra fact sheet" below)
- A sheet of information is printed on the reverse with some random facts about groups related to, and which contains several important facts about, cyclic groups.
- Every finite abelian group G is a direct sum of groups $\mathbb{Z}_{p^k}$ for prime p. The p^k are called the *elementary divisors* of G.
- The direct sum $\oplus_{k=1}^{N} \mathbb{Z}_{m_k} = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_N}$ is cyclic iff the gcd of any pair of the m_k is 1.
- The order of a subgroup divides into order of group.
- A nonzero m in $\mathbb{Z}_n$ is a zero divisor iff $\gcd(m, n) \neq 1$, so $\mathbb{Z}_n$ is an integral domain iff n is prime.
- An ideal in a ring R is an additive subgroup I with $RIR \subset I$.
- The ideals in Z_n are precisely $\langle k \rangle$ where k divides n. An ideal I in Z_n is maximal if and only if $I = \langle p \rangle$ where p is a prime dividing n.
- Every finite integral domain is a field, so every nonzero element is a *unit* (that is, has a multiplicative inverse).
- A number is divisible: By 2: if the units digit is 0,2,4,6,8.
  By 3: if the sum of all digits is a multiple of 3.
  By 4: if the last two digits form a number that's a multiple of 4.
  By 5: if the units digit is 0 or 5
  By 6: if divisible by both 2 and 3.
  By 8: of last 3 digits form a number divisible by 8.
  By 9: if the sum of the digits is a multiple of 9.
- Notation: $f(A) = \{f(x) : x \in A\}, f^{-1}(A) = \{x \in \text{dom}(f) : f(x) \in A\}$. Injective (1-1), surjective (onto), bijective (1-1 onto)
- An integral domain is a nonzero commutative ring without zero-divisors. Eg. a field.

Major Facts about Cyclic Groups

Theorem 1. (**Criterion for $a^i = a^j$**) Let G be a group and $a \in G$.

a. If $|a| = \infty$, then all distinct powers of a are distinct group elements of G;

b. If $|a| = n$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$
and $a^i = a^j$ if and only if $n \mid (i - j)$.

Corollary 1.1. For any $a \in G$, $|a| = |\langle a \rangle|$.

Corollary 1.2. Let $a \in G$ such that $|a| = n$. If $a^k = e$ for some k, then $n \mid k$.

Theorem 2. Let $a \in G$ such that $|a| = n$ and let $k > 0$.
Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n, k)$.

Corollary 2.1. (**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 $\gcd(n, i) = \gcd(n, j)$.

Corollary 2.2. (**Generators of Cyclic Groups**) Let $G = \langle a \rangle$ be a cyclic group of order n.
Then $G = \langle a^k \rangle$ if and only if $\gcd(n, k) = 1$.

Corollary 2.3. (**Generators of $\mathbb{Z}_n$**) k is a generator of $\mathbb{Z}_n$ if and only if $\gcd(n, k) = 1$.

Theorem 3. (**Fundamental Theorem of Cyclic Groups**) Let $G = \langle a \rangle$ be a cyclic group.
Then

a. Every subgroup of G is cyclic;

b. If $|G| = n$, then the order of any subgroup of G divides n;

c. For each positive divisor k of n, the group G has exactly one subgroup of order k, that is, $\langle a^{n/k} \rangle$.

Corollary 3.1. (**Subgroups of $\mathbb{Z}_n$**) For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. Moreover, these are the only subgroups of $\mathbb{Z}_n$.

Algebra fact sheet (Taken from MIT website)

An **algebraic structure** (such as group, ring, field, etc.) is a set with some operations and distinguished elements (such as $0, 1$) satisfying some axioms. This is a fact sheet with definitions and properties of some of the most important algebraic structures.

A **substructure** of a structure A (i.e., a subgroup, subring, subfield etc.) is a subset of A that is closed under all operations and contains all distinguished elements.

Algebraic structures of the same type (e.g., groups) can be related to each other by homomorphisms. A **homomorphism** $f : A \to B$ is a map that preserves all operations and distinguished elements (e.g. $f(ab) = f(a)f(b)$). An **isomorphism** is a homomorphism which is a one-to-one correspondence (bijection); then the inverse f^{-1} is also an isomorphism. Isomorphic algebraic structures are regarded as the same, and algebraic structures of each type are classified up to an isomorphism. An automorphism is an isomorphism $f: A \to A$.

Semigroup: A set G with an operation $G \times G \to G$, $(a, b) \mapsto ab$, called multiplication, which is associative: $(ab)c = a(bc)$.

Examples: Positive integers with operation of addition.

Monoid: A semigroup G with unit $1 \in G$, such that $1g = g1 = g$ for all $g \in G$.

Note that a unit is unique: $1 = 11' = 1'$.

Examples: Nonnegative integers under addition; all integers under multiplication.

Group: A monoid G with an inversion operation $G \to G$, $g \mapsto g^{-1}$, such that $gg^{-1} = g^{-1}g = 1$.

Note that inverse is unique: $g_1^{-1} = g_1^{-1}gg_2^{-1} = g_2^{-1}$. So for a semigroup, being a monoid or a group is a property, not an additional structure.

Examples: (1) All integers under addition, $\mathbf{Z}$. Integers modulo n under addition, $\mathbf{Z}_n$. (These two are called cyclic groups). The group $\mathbf{Z}^N$ (N-dimensional vectors of integers). Rational numbers $\mathbf{Q}$, real numbers $\mathbf{R}$, or complex numbers $\mathbf{C}$ under addition. Nonzero rational, real, or complex numbers under multiplication.

(2) Permutation (or symmetric) group S_n on n items. The group GL_n of invertible matrices with integer, rational, real, or complex entries, or with integer entries modulo n (e.g. $GL_n(\mathbf{Q})$). The group of symmetries of a polytope (e.g., regular icosahedron).

Abelian (commutative) group: A group G where $ab = ba$ (commuta-

tivity).

Examples: The examples from list (1) above.

If A is an abelian group, one often denotes the operation by $+$ and 1 by 0.

Action of a monoid or a group on a set: A left action of a monoid (in particular, a group) G on a set X is a multiplication map $G \times X \to X$, $(g, x) \mapsto gx$ such that $(gh)x = g(hx)$ and $1x = x$. Similarly one defines a right action, $(x, g) \mapsto xg$.

Examples. Any monoid (in particular, group) acts on itself by left and right multiplication. The symmetric group S_n acts on $\{1, ..., n\}$. Matrices act on vectors. The group of symmetries of a regular icosahedron acts on the sets of its points, vertices, edges, faces and on the ambient space.

Normal subgroup: A subgroup $H \subset G$ such that $gH = Hg$ for all $g \in G$.

Quotient group: If A is an abelian group and B a subgroup in A, then A/B is the set of subsets aB in A (where $a \in A$) with operation $a_1Ba_2B = a_1a_2B$; this defines a group structure on A/B. If A is not abelian, then in general A/B is just a set with a left action of A. For it to be a group (i.e., for the formula $a_1Ba_2B = a_1a_2B$ to make sense), B needs to be a normal subgroup. This is automatic for abelian groups A.

Examples. $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$. $S_3/\mathbf{Z}_3 = \mathbf{Z}_2$.

Lagrange's theorem: The order (i.e., number of elements) of a subgroup H of a finite group G divides the order of G (the quotient $|G|/|H|$ is $|G/H|$).

The **order** of $g \in G$ is the smallest positive integer n such that $g^n = 1$ (∞ if there is none). Equivalently, the order of g is the order of the subgroup generated by g. Thus by Lagrange's theorem, the order of g divides the order of G. This implies that any group of order p (a prime) is $\mathbf{Z}_p$.

Direct (or Cartesian) product (of semigroups, monoids, groups): $G \times H$ is the set of pairs (g, h), $g \in G, h \in H$, with componentwise operation.

One can also define a direct product of more than two factors. For abelian groups, the direct product is also called the direct sum and denoted by $\oplus$.

Generators: A group G is generated by a subset $S \subset G$ if any element of G is a product of elements of S and their inverses. A group is finitely generated if it is generated by a finite subset.

Classification theorem of finitely generated abelian groups. Any finitely generated abelian group is a direct sum of infinite cyclic groups ($\mathbf{Z}$)

and cyclic groups of prime power order. Moreover, this decomposition is unique up to order of factors (and up to isomorphism).

(Unital) ring: An abelian group A with operation $+$ which also has another operation of multiplication, $(a, b) \mapsto ab$, under which A is a monoid, and which is distributive: $a(b + c) = ab + ac$, $(b + c)a = ba + ca$.

Examples: (1) The integers $\mathbf{Z}$. Rational, real, or complex numbers. Integers modulo n ($\mathbf{Z}_n$). Polynomials $\mathbf{Q}[x], \mathbf{Q}[x, y]$.

(2) Matrices n by n with rational, real, or complex entries, e.g. $\mathrm{Mat}_n(\mathbf{Q})$.

Commutative ring: A ring in which $ab = ba$.

Examples: List (1) of examples of rings.

Division ring: A ring in which all nonzero elements are invertible (i.e., form a group).

Examples: Rational, real, complex numbers. Integers modulo a prime ($\mathbf{Z}_p$). Quaternions.

Field: A commutative division ring.

Examples: Rational, real, complex numbers. Integers modulo a prime ($\mathbf{Z}_p$). Finite fields have order p^k, p prime.

Characteristic of a field F: The smallest positive integer p such that $1 + ... + 1$ (p times) is zero in F. If there is no such p, the characteristic is said to be zero. If the characteristic is not zero then it is a prime.

Examples: The characteristic of $\mathbf{Z}_p$ is p. The characteristic of $\mathbf{Q}$ is zero.

Unital **Algebra over a field F:** A ring A containing F such that elements of F commute with all elements of A. [Or: a ring that is also a vector space such that....]

Examples: $\mathbf{Q}[x], \mathbf{Q}[x, y]$, $\mathrm{Mat}_2(\mathbf{Q})$ (2 by 2 matrices with rational enties) are algebras over $\mathbf{Q}$.

(Left) module over a ring A: An abelian group M with a multiplication $A \times M \to M$, $(a, m) \mapsto am$ which is associative ($(ab)m = a(bm)$) and distributive ($a(m_1 + n_2) = am_1 + am_2, (a_1 + a_2)m = a_1m + a_2m$), and such that $1m = m$ (i.e., the monoid A acts on M, and the action is distributive in both arguments). Similarly one defines right modules (with multiplication $(m, a) \mapsto ma$). Note that for a commutative ring, a left module is the same thing as a right module.

Examples: A module over $\mathbf{Z}$ is the same thing as an abelian group. Also, for any ring A, $A^n = A \oplus ... \oplus A$ (n times) is a module over A, left and right (called free module of rank n). More generally, if S is a set, then the **free A-module** $A[S]$ with basis S is the set of formal finite sums $\sum_{s \in S} a_s s$, $a_s \in A$, where all a_s but finitely many are zero.

Idempotent: $a^2 = a$

Nilpotent: $a^k = 0$ for some $k \in \mathbb{N}$.