PMATH352W18 Cheatsheet
by Johnson Ng, page 1 of 1

Injectivity Let $f : X \to Y$ be a function. We say that f is *injective* (or *one-to-one*) if $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

Surjectivity Let $f : X \to Y$ be a function. We say that f is *surjective* (or *onto*) if $\forall y \in Y \;\; \exists x \in X \;\; f(x) = y$.

Bijectivity Let $f : X \to Y$ be a function. We say that f is *bijective* if it is both *injective* and *surjective*.

Permutations Given a non-empty set L, a permutation of L is a bijection from L to L. The set of all permutations of L is denoted by S_L.

Order The *order* of a set A, denoted by $|A|$, is the cardinality of the set.

Groups Let G be a set and $*$ an operation on $G \times G$. We say that $G = (G, *)$ is a *group* if it satisfies

1. *Closure*: $\forall a, b \in G \quad a * b \in G$
2. *Associativity*: $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$
3. *Identity*: $\exists e \in G \; \forall a \in G \quad a * e = a = e * a$
4. *Inverse*: $\forall a \in G \; \exists b \in G \quad a * b = e = b * a$

Abelian Group A group G is said to be abelian if $\forall a, b \in G$, we have $a * b = b * a$.

General Linear Group The *general linear group of degree n over $\mathbb{R}$* is defined as

$$GL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}) \, : \, \det M \neq 0\}$$

Cayley Table Let G be a group. Given $x, y \in G$, let the product xy be an entry of a table in the row corresponding to x and column corresponding to y. Such a table is called a *Cayley Table*.

Subgroup Let G be a group and $H \subseteq G$. If H itself is a group, then we say that H is a subgroup of G

Special Linear Group The *special linear group* of order n of $\mathbb{R}$ is defined as

$$\begin{aligned} SL_n(\mathbb{R}) &= (SL_n(\mathbb{R}), \cdot) \\ &= \{A \in M_n(\mathbb{R}) : \det A = 1\} \end{aligned}$$

Center of a Group Given a group G, the *the center of a group* G is defined as

$$Z(G) = \{z \in G \, : \, \forall g \in G \;\; zg = gz\}$$

Transposition A *transposition* $\sigma \in S_n$ is a cycle of length 2, i.e. $\sigma = (a \;\; b)$, where $a, b \in \{1, ..., n\}$ and $a \neq b$.

Odd and Even Permutations A permutation σ is even (or odd) if it can be written as a product of an even (or odd) number of transpositions. By the *Parity Theorem*, a permutation must either be even or odd, but not both.

Cyclic Groups Let G be a group and $g \in G$. Then we call $\langle \, g \, \rangle$ the *cyclic subgroup* of G generated by g. If $G = \langle \, g \, \rangle$ for some $g \in G$, then we say that G is a *cyclic group*, and g is a *generator* of G.

Order of an Element Let G be a group and $g \in G$. If n is the smallest positive integer such that $g^n = 1$, we say that the order of g is n, denoted by $o(g) = n$.
If no such n exists, then we say that g has infinite order and write $o(g) = \infty$.

Dihedral Group Recall from Assignment 1 that the dihedral group is a set of rigid motions for transforming a regular polygon back to its original position while changing the index of its vertices. For $n \geq 2$, the *dihedral group* of order $2n$ is

$$D_{2n} = \{1, a, ..., a^{n-1}, b, ba, ..., b^{n-1}\}$$

where $a^n = 1 = b^2$ and $aba = b$. Note that a represents a rotation of $\frac{2\pi}{n}$ radians, and b represents a reflection through the x-axis

Group Homomorphism Let G, H be groups. A mapping

$$\alpha : G \to H$$

is called a group *homomorphism* if $\forall a, b \in G$, Note that ab uses the operation of G while $\alpha(a)\alpha(b)$ uses the operation of H.

$$\alpha(ab) = \alpha(a)\alpha(b).$$

Isomorphism Let G, H be groups. Consider a mapping

$$\alpha : G \to H$$

We say that α is an *isomorphism* if it is a homomorphism and bijective.
If α is an isomorphism, we say that G is *isomorphic to* H, or that G and H are *isomorphic*, and denote that by $G \cong H$.

Coset Let H be a subgroup of a group G.

$$\forall a \in G \quad Ha = \{ha : h \in H\}$$

is the right coset of H generated by a and

$$\forall a \in G \quad aH = \{ah : h \in H\}$$

is the left coset of H generated by a.

Normal Subgroup Let H be a subgroup of a group G. If $\forall g \in G$, we have $Hg = gH$, then we say that H is a *normal subgroup* of G, and write

$$H \triangleleft G$$

Product of Groups

$$HK := \{hk \, : \, h \in H, \, k \in K\}$$

Normalizer Let H be a subgroup of G. The *normalizer of* H, denoted by $N_G(H)$, is defined to be

$$N_G(H) := \{g \in G \, : \, gH = Hg\}$$

Quotient Group Let $K \triangleleft G$. The group GK of all cosets of K in G is called the *quotient group* of G by K. Also, the mapping

$$\phi : G \to GK \text{ defined by } a \mapsto Ka$$

is called the *coset* (or *quotient*) *map*.

Kernel and Image Let $\alpha : G \to H$ be a group homomorphism. The *kernel* of α is defined by

$$\ker \alpha := \{g \in G \, : \, \alpha(g) = 1_H\} \subseteq G$$

and the image of α is defined by

$$\operatorname{im} \alpha := \alpha(G) = \{\alpha(g) \, : \, g \in G\} \subseteq H.$$

Group Action Let G be a group, X a non-empty set. A *group action* of G on X is a mapping $G \times X \to X$ denoted as $(a, x) \to ax$ such that

1. $1 \cdot x = x, \; x \in X$
2. $a \cdot (b \cdot x) = (ab) \cdot x, \; a, b \in G, \; x \in X$

In this case, we say G *acts on* X.

Orbit & Stabilizer Let G be a group acting on a set X, and $x \in X$. We denote by

$$G \cdot x = \{g \cdot x : \forall g \in G\}$$

the *orbit* of x and

$$S(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

the *stabilizer* of x.

p-Group Let p be a prime. A *p-group* is a group in which every element has an order that is a non-negative power of p.

Ring A set R is a ring if $\forall a, b, c \in R$,

1. $a + b \in R$
2. $a + b = b + a$
3. $a + (b + c) = (a + b) + c$
4. $\exists 0 \in R \;\; a + 0 = a = 0 + a$
5. $\exists (-a) \in R \;\; a + (-a) = 0 = (-a) + a$
6. $ab \in R$
7. $a(bc) = (ab)c$
8. $\exists 1 \in R \;\; 1 \cdot a = a = a \cdot 1$
9. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

We call 1 as the *Unity* of R, 0 as the *Zero* of R, and $-a$ as the *negative* of a.
The ring R is called a *Commutative Ring* if it also satisfies the following:

10. $ab = ba$.

Trivial Ring A *trivial ring* is a ring of only one element. In this case, we have $1 = 0$, i.e. the unity is the zero and vice versa.

Characteristic of a Ring If R is a ring, we define the *characteristic* of R, denoted by $\operatorname{ch}(R)$, in terms of the order of 1_R in the additive group $(R, +)$, by

$$\operatorname{ch}(R) = \begin{cases} n & \text{if } o(1_R) = n \in \mathbb{N} \\ 0 & \text{if } o(1_R) = \infty \end{cases}$$

Subring A subset S of a ring R is a subring if S is a ring itself (under the same operations: addition and multiplication).

Ideal An additive subgroup A of a ring R is called an *ideal* of R if $Ra, aR \subseteq A$, $\forall a \in A$.

Quotient Ring Let A be an ideal of a ring R. Then the ring RA is called the *quotient ring* of R by A.

Principal Ideal Let R be a commutative ring and A an ideal of R. If $A = aR = \{ar : r \in R\} = Ra$ for some $a \in A$, we say that A is a *principal ideal* *generated* by a, and denote $A = \langle \, a \, \rangle$.

Ring Homomorphism Let R and S be rings. A mapping

$$\Theta : R \to S$$

is a ring *homomorphism* if $\forall a, b \in R$, we have

1. $\Theta(a + b) = \Theta(a) + \Theta(b)$
2. $\Theta(ab) = \Theta(a)\Theta(b)$
3. $\Theta(1_R) = 1_S$

Ring Isomorphism A mapping of rings $\Theta : R \to S$ is a ring *isomorphism* if Θ is a bijective ring homomorphism. In this case, we say that R and S are *isomorphic* and denote that by $R \cong S$.

Kernel and Image Let $\Theta : R \to S$ be a ring homomorphism. The *kernel* of Θ is defined by

$$\ker \Theta = \{r \in R : \Theta(r) = 0_S\}$$

and the *image* of Θ is defined by

$$\operatorname{im} \Theta := \Theta(R) = \{\Theta(r) : r \in R\}.$$

Units Let R be a ring. We say that $u \in R$ is a *unit* if u has a multiplicative inverse in R, and denote it by u^{-1}. We have

$$uu^{-1} = 1 = u^{-1}u$$

Division Ring and Field A non-trivial ring R is a *division ring* if

$$R^* = R \setminus \{0\}.$$

A commutative division ring is a *field*.

Zero Divisor Let R be a non-trivial ring. If $0 \neq a \in R$, then a is called a *zero divisor* if $\exists 0 \neq b \in R$ such that $ab = 0$.

Integral Domain *A commutative ring $R \neq \{0\}$ (i.e. non-trivial ring) is called an integral domain if it has no zero divisor, i.e. if $ab = 0 \in R$ then $a = 0$ or $b = 0$.*

Prime Ideals *Let R be a commutative ring. An ideal $P \neq R$ is a prime ideal of R if $r, s \in R$ satisfy: $rs \in P \implies r \in P$ or $s \in P$.*

Maximal Ideals *Let R be a (commutative) ring. An ideal $M \neq R$ or R is a maximal ideal if $\forall A$ that is an ideal of R, we have that*

$$M \subseteq A \subseteq R \implies A = M \text{ or } A + R.$$

Fraction *Let R be an integral domain, $D = R \setminus \{0\}$, and $X = R \times D$. The fraction, $\frac{r}{s}$ to be the equivalent class $[(r, s)]$ of the pair $(r, s) \in X$.*

Polynomials *Let R be a ring and x a variable. Let*
$R[x] = \left\{ f(x) = \sum_{i=0}^{m} a_i x^i : m \in \mathbb{N} \cup \{0\}, a_i \in R, 0 \leq i \leq m \right\}$.
Each element in $R[x]$ is called a polynomial in x over R. If $a_m \neq 0$, we say that $f(x)$ has degree m, denoted by $\deg f = m$, and we say that a_m is the leading coefficient of $f(x)$.
If $\deg f = 0$, then $f(x) = a_0 \in R$. In this case, we call $f(x)$ a constant polynomial. Note if

$$f(x) = 0 \iff a_0 = a_1 = ... = a_m = 0,$$

we define $\deg 0 = -\infty$, and $f(x)$ is called a zero polynomial.

Division of Polynomials *Let R be a commutative ring and $f(x), g(x) \in R[x]$. We say that $f(x)$ divides $g(x)$, denoted as $f(x) \mid g(x)$ if $\exists q(x) \in R[x]$ such that*

$$g(x) = q(x)f(x)$$

Monic Polynomial *Let R be a commutative ring and $f(x) \in R[x]$. $f(x)$ is monic if its leading coefficient is 1.*

Irreducible Polynomials *Let F be a field. A non-zero polynomial $l(x) \in F[x]$ is irreducible if $\deg l \geq 1$ and if*

$$l(x) = l_1(x)l_2(x)$$

for $l_1(x), l_2(x) \in F[x]$, then $\deg l_1 = 0$ or $\deg l_2 = 0$ Note that polynomials of degree 0 are the units of $F[x]$.. Polynomials that are not irreducible are called reducible polynomials.

Division *Let R be an integral domain and $a, b \in R$. We say that $a \mid b$ if $b = ca$ for some $c \in R$.*

Association *Let R be an integral domain. $\forall a, b \in R$, we say that a is associated to b, denoted by $a \sim b$, if $a \mid b$ and $b \mid a$.*

Irreducible *Let R be an integral domain. We say $p \in R$ is irreducible if $p \neq 0$ is not a unit, and $p = ab \in R$, then either a or b is a unit. An element that is not irreducible is reducible.*

Prime *Let R be an integral domain and $p \in R$. We say p is prime in R if $p \neq 0$ is not a unit, and if $p \mid ab \in R \implies p \mid a \veebar p \mid b$.*

Ascending Chain Condition on Principal Ideals (ACCP) *An integral domain R is said to satisfy the ascending chain condition on principal ideals (ACCP) if for any ascending chain*

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \ldots$$

of principal ideals in R, $\exists n \in \mathbb{N}$ such that

$$\langle a_n \rangle = \langle a_{n+1} \rangle = \ldots .$$

Unique Factorization Domain (UFD) *An integral domain R is called a unique factorization domain (UFD) if it satisfies the following conditions:*

1. *If $0 \neq a \in R$ is a non-unit, then a is a product of irreducible elements in R.*
2. *If $p_1 p_2 \ldots p_r \sim q_1 q_2 \ldots q_s$ where p_i and q_i are irreducibles, then $r = s$ and (possibly after relabelling) $p_i \sim q_i$ for each $1 \leq i \leq r = s$.*

Greatest Common Divisor *Let R be an integral domain, and $a, b \in R$. We say $d \in R$ is the greatest common divisor of a, b, denoted as $\gcd(a, b) = d$, if it satisfies the following conditions:*

1. *$d \mid a$ and $d \mid b$;*
2. *$e \in R$ $e \mid a \wedge e \mid b \implies e \mid d$.*

Principal Ideal Domain (PID) *An integral domain R is a principal ideal domain (PID) if every ideal is principal.*

Content *If R is a UFD and if $0 \neq f(x) \in R[x]$, the greatest common divisor of the non-zero coefficients of $f(x)$ is called the content of $f(x)$, and denoted by $\mathrm{c}(f)$.*

Primitive Polynomials *If R is a UFD and if $0 \neq f(x) \in R[x]$, then if $\mathrm{c}(f) \sim 1$, we say that $f(x)$ is a primitive polynomial, or simply say that $f(x)$ is primitive.*