MA2202
AY22/23 Sem 2
Wong Kai Jie
Adapted from `https://github.com/jovyntls/cheatsheets`

BASIC NUMBER THEORY

Definition. A nonzero $p \in \mathbb{Z}$ is **prime** if

(i) $p \neq \pm 1$, and
(ii) if $p|ab$ for some $a, b \in \mathbb{Z}$, then $p|a$ or $p|b$.

Definition. A nonzero $p \in \mathbb{Z}$ is **irreducible** if

(i) $p \neq \pm 1$, and
(ii) if $p = xy$ for some $x, y \in \mathbb{Z}$, then $x = \pm 1$ or $y = \pm 1$.

Division Algorithm
Let $x, y \in \mathbb{Z}$ with $y \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$x = qy + r, 0 \leq r < |y|.$$

Properties of gcd(x,y):
- $\gcd(0, y) = |y|$
- $\gcd(x, y) = \gcd(x, |y|)$
- $\gcd(cx, cy) = |c| \gcd(x, y)$
- $\gcd(x, y) = \gcd(x + y, y) = \gcd(x - y, y)$
- $\gcd(x, y) = \gcd(y, r)$

Bezout's Identity
$\gcd(a, b) = ax + by$, for some $x, y \in \mathbb{Z}$.
Note if $d = \gcd(x, y)$, $d\mathbb{Z} = \{mx + ny \in \mathbb{Z} : m, n \in \mathbb{Z}\}$

Linear congruences

Definition. For $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod{m}$ if $m|(a - b)$.

Fermat's Little Theorem (cf. Euler's Theorem)
Given a positive prime integer p and $n \in \mathbb{Z}$, we have $n^p \equiv n \pmod{p}$.

Theorem. *Suppose* $\gcd(a, m) = 1$. *Then for* $b \in \mathbb{Z}$,

$$ax \equiv b \pmod{m}$$

has a unique solution modulo m.

Chinese Remainder Theorem
Suppose $\gcd(m, n) = 1$. Then the system of congruences

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

has a unique solution modulo mn.
Verify that one solution is $x = anz + bmy$, where $my + nz = 1$.

GROUPS

Definition. A **group** $(G, *)$ consists of a set G and a binary operation $*$ on G which satisfy the following axioms:
- (G1) (Closure) For all $a, b \in G, a * b \in G$.
- (G2) (Associativity) For all $a, b, c \in G$,

$$(a * b) * c = a * (b * c).$$

- (G3) (Existence of identity) There exists an element $e \in G$, such that for all $a \in G$,

$$e * a = a * e = a.$$

- (G4) (Existence of inverse) For each $a \in G$, there exists an element $b \in G$ such that

$$a * b = b * a = e.$$

Note:
- The identity element e is unique in G.
- The inverse of an element is unique.
- $(a * b)^{-1} = b^{-1} * a^{-1}$.
- $\forall n \in \mathbb{Z}, (a^n)^{-1} = (a^{-1})^n$.
- $\forall n \in \mathbb{Z}, a^n * a^m = a^{n+m}$.
- (Right Cancellation Law) $a * c = b * c \Rightarrow a = b$.
- (G1), (G2), (RG3) and (RG4) are sufficient to define a group G.
  - (RG3) (Existence of right identity) There exists an element $e \in G$, such that for all $a \in G, a * e = a$.
  - (RG4) (Existence of right inverse) For each $a \in G$, there exists an element $b \in G$ such that $a * b = e$.

Examples of groups

- Let G be a vector space over a field F and let $+$ be the addition of vectors. Then $(G, +)$ is an abelian group.
- $(\mathbb{Q}^\times, \times), (\mathbb{R}^\times, \times), (\mathbb{C}^\times, \times)$ are abelian groups.

n-th roots of unity in $\mathbb{C}$
Given $n \in \mathbb{Z}^+$, define

$$\mu_n = \{e^{\frac{2k\pi i}{n}} : k = 0, 1, \ldots, n - 1\}$$

Then $(\mu_n, \times)$ is the **cyclic group** of order n.

Klein four-group
$\mu_2 \times \mu_2$ forms a group of order 4.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Group isomorphisms

Definition. Let $(G, *)$ and $(H, \star)$ be two groups. If a homomorphism $\phi \colon G \to H$ is bijective, it is a **group isomorphism**. We denote $(G, *) \simeq (H, \star)$.

Note:
- ϕ^{-1} is a group isomorphism
- Composing isomorphisms gives an isomorphism

Subgroups

Definition. Let $(G, *)$ be a group. Let $H \subseteq G$ be a nonempty subset. Suppose $(H, *)$ forms a group. Then, $(H, *)$ is a subgroup of $(G, *)$.

Note:
- $(I, +)$ is a subgroup of $(\mathbb{Z}, +) \Leftrightarrow I = d\mathbb{Z}$ for some non-negative integer d.
  - In particular, if $d \neq 0$, d is the smallest positive integer in I.
- $(\mu_m, \times)$ is a subgroup of $(\mu_n, \times) \Leftrightarrow m|n$.
- $(H, *)$ is a subgroup if and only if:
  - (S1) For all $a, b \in H$, we have $a * b \in H$.
  - (S2) For all $a \in H$, we have $a^{-1} \in H$.
- Alternatively:
  - (S) For all $a, b \in H$, we have $a * b^{-1} \in H$.
- For nonempty finite subset H, (S1) is sufficient.
- If $\{(H_i, *) : i \in I\}$ is a collection of subgroups of $(G, *)$, then

$$(\bigcap_{i \in I} H_i, *)$$

  is a subgroup of $(G, *)$.

SYMMETRIC GROUPS

Definition. Let $X = \{1, 2, \ldots, n\}$ and

$$S_n = \{f \colon X \to X : f \text{ is a bijection.}\}.$$

The pair $(S_n, \circ)$ is called the **symmetric group** or **permutation group** on n letters.

A general element $k \in S_n$ could be denoted by

$$k = \begin{pmatrix} 1 & 2 & \ldots & n \\ k(1) & k(2) & \ldots & k(n) \end{pmatrix}$$

For any arbitrary set $Y = \{y_1, y_2, \ldots, y_n\}$, we denote

$$S_Y = \{f \colon Y \to Y : \text{ f is a bijection.}\}.$$

Then $(S_n, \circ) \simeq (S_Y, \circ)$.

- Explicitly, let $T \colon X \to Y$ be the bijection given by $T(i) = y_i$. Then $\phi \colon S_n \to S_Y$ given by

$$\phi(f) = T \circ f \circ T^{-1}$$

  is an isomorphism.

Permutation matrices

Definition. Let $\{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$ be the standard basis of $\mathbf{R}^n$. An n by n **permutation matrix** is a matrix of the form

$$F = \begin{pmatrix} | & | & \ldots & | \\ \mathbf{e}_{i_1} & \mathbf{e}_{i_2} & \ldots & \mathbf{e}_{i_n} \\ | & | & \ldots & | \end{pmatrix}$$

where $\{\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}\}$ is a permutation of the standard basis vectors.
Let S_n'' be the set of all n by n permutation matrices. Then $(S_n'', \times)$ forms a group, where $(S_n'', \times) \simeq (S_n, \circ)$.

Note:
- $det(F) = \pm 1$.
- $\forall f \in S_n, sgn(f) = det(\phi(f))$ where ϕ is the obvious group isomorphism $S_n \to S_n''$.

Cyclic notations

Let $f \in S_n$. Then
(i) $f = h_1 \circ h_2 \circ \ldots \circ h_r$ can be factorised into a product of mutually disjoint cycles.
(ii) The factorisation in (i) is unique up to an ordering of the product of cycles.

Note:
- If h, h' are disjointed cycles, $h \circ h' = h' \circ h$.
- Let $c = (i_1 i_2 \ldots i_r)$ and $f \in S_n$. Then

$$f \circ c \circ f^{-1} = (f(i_1) f(i_2) \ldots f(i_r)).$$

  In particular, it is an r-cycle.
- $c^{-1} = (i_r i_{r-1} \ldots i_1)$.
- Let $f = c_1 c_2 \ldots c_k \in S_n$ where c_i are mutually disjointed cycles of orders r_i. Then
  - $f^m = c_1^m c_2^m \ldots c_k^m$.
  - $f^m = e \Leftrightarrow lcm(r_1, r_2, \ldots, r_k)|m$.

Transpositions

Definition. A cycle $h \in S_n$ of the form $h = (ij)$ is called a **transposition**.

Note:
- $(i_1 \ldots i_r) = (i_1 i_r)(i_1 i_{r-1}) \ldots (i_1 i_2)$
- For any $f \in S_n$, f is a product of transpositions.
  - In particular, $(i_1 i_2 \ldots i_r) = (i_1 i_r)(i_1 i_{r-1}) \ldots (i_1 i_3)(i_1 i_2)$.
- $(ab)(cd) = (acb)(cda)$. Thus every even permutation in S_n is a product of 3-cycles.

Sign character

Let $f \in S_n$. Define the polynomials

$$P(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j),$$

$$P_f(x_1, \ldots, x_n) = P(x_{f(1)}, \ldots, x_{f(n)})$$

Then we write

$$P_f(x_1, \ldots, x_n) = sgn(f) P(x_1, \ldots, x_n)$$

where $sgn(f) = \pm 1$. Note that $sgn(f \circ h) = sgn(f) sgn(h)$. An element $f \in S_n$ is called an *even* (respectively *odd*) permutation if $sgn(f) = 1$ (respectively $sgn(f) = -1$).

SYMMETRIC GROUPS (cont'd)

Note:
- A transposition is an odd permutation, i.e. $sgn(ij) = -1$.
- $f \in S_n$ is even $\Leftrightarrow$ f is a produce of an even number of transpositions.

Alternating group

Define the alternating group A_n as

$$A_n = \{f \in S_n : sgn(f) = 1\} = \{f \in S_n : f \text{ even}\}.$$

Then $(A_n, \circ)$ is a subgroup of $(S_n, \circ)$.
- $|A_n| = n!/2$.
- Let H be a subgroup of S_n which contains all the 3-cycles of S_n. Then H is either A_n or S_n.

Cayley's Theorem

Every finite group $(G, *)$ of order n is isomorphic to a subgroup of $(S_n, \circ)$.
- Let $(\mu_p, \times)$ be the cyclic subgroup of order p, where p is prime. If $(\mu_p, \times)$ is isomorphic to a subgroup of S_m, then $p \le m$.

LAGRANGE'S THEOREM

Cosets

Let G be a group and H be a subgroup. Let $x, y, z \in G$.
- If $z \in xH$, then $zH = xH$.
- If $xH \cap yH \neq \emptyset$, then $xH = yH$.
- The left cosets $\{xH : x \in G\}$ form a partition of G.
- For every coset xH is of the same cardinality as H.
- $k\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, and for $a \in \mathbb{Z}$, the cosets $a + k\mathbb{Z}$ form a disjointed union

$$\mathbb{Z} = k\mathbb{Z} \bigsqcup (1 + k\mathbb{Z}) \bigsqcup \ldots \bigsqcup (k - 1 + k\mathbb{Z})$$

- If H, K are subgroups of G, and $x \in G$, then $x(H \cup K) = xH \cup xK$.
  - Let $x, y \in G$. Then $xH \cup yK$ is either the empty set or equal to $c(H \cup K)$ for some $c \in G$.

Lagrange's Theorem

Let G be a finite group and H be a subgroup. Then $|H|$ divides $|G|$.
Furthermore $[G : H] = |G/H| = |G|/|H|$.

GENERATORS OF GROUPS

Let G be a group and X be a subset of G.

Definition. Let $S = \{H : H \text{ subgroup of } G, X \subseteq H\}$. We define

$$\langle X \rangle = \bigcap_{H \in S} H.$$

as the subgroup of G *generated* by X.
- $\langle X \rangle$ is the *smallest subgroup* of G containing X.
- We say that a group is *finitely generated* if it is generated by some finite subset.

Definition. A *word* on X is either e or a finite product $x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n} \in G$ where $x_i \in X$ and $r_i \in \mathbb{Z}$. Let W be the set of words on X. Then $W = \langle X \rangle$.

Cyclic groups

Let G be a group and $a \in G$.
- Denote $o(a) = r$, where r is the smallest positive integer such that $a^r = e$.
- $\langle a \rangle = \{e, a, a^2, \ldots, a^{r-1}\}$ is a cyclic group of order r.
- If G is a finite group of order p where p is prime. If $a \neq e$, then $G = \langle a \rangle$.

HOMOMORPHISMS

Definition. Let $(G, *)$ and $(H, \star)$ be two groups. A function $\phi \colon G \to H$ is called a **group homomorphism** if

$$\phi(x * y) = \phi(x) \star \phi(y)$$

for all $x, y \in G$.

Note:
- Composing homomorphisms gives a homomorphism.
- $\phi(e_G) = e_H$.
- $\phi(g^{-1}) = \phi(g)^{-1}$
- The image $\phi(G)$ is a subgroup of $(H, \star)$.
- Let H' be a subgroup of H. Then $\phi^{-1}(H')$ is a subgroup of G.

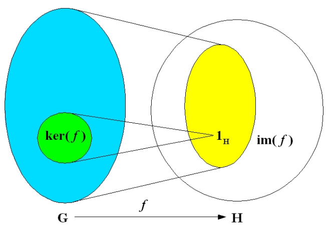
Definition. The **kernel** of ϕ is defined as

$$\ker \phi = \phi^{-1}(e_H) = \{g \in G : \phi(g) = e_H\}.$$

Note:
- The kernel K is a *normal* subgroup of G.
- For all $g_0 \in G$, we have

$$\{g \in G : \phi(g) = \phi(g_0)\} = g_0 K = K g_0.$$

- Thus ϕ injective $\Leftrightarrow$ $ker\phi = \{e_G\}$.



Definition. Let $K = \ker \phi$ be the kernel of ϕ. We define

$\mathbf{Sub}(G, K) = \{G' : G' \text{ subgroup of } G, K \subseteq G\}$ and

$\mathbf{Sub}(H) = \{H' : H' \text{ subgroup of } H\}$.

We define a function $\Phi \colon \mathbf{Sub}(G, K) \to \mathbf{Sub}(H)$ by $\Phi(G') = \phi(G')$ where $G' \in \mathbf{Sub}(G, K)$.
- If ϕ is a **surjective** homomorphism, then Φ is a bijection.
  - Verify that Φ is well-defined.

NORMAL SUBGROUPS

Definition. Let G be a group and N be a subgroup. Then $N \lhd G$ if for all $n \in N$ and $g \in G$, $gng^{-1} \in N$.
- $\bigcap_{i \in I} N_i$ is a normal subgroup of G.
- For every subgroup G' of G, $N \cap G'$ is a normal subgroup of G.

The following statements are equivalent:
1. (i) The subgroup N is normal, i.e. $\forall n \in N, g \in G, gng^{-1} \in N$.
2. (ii) For all $g \in G, gNg^{-1} = N$.
3. (iii) For all $g \in G, gN = Ng$.
4. (iv) For all $g, g' \in G, (gN)(g'N) = (gg')N$.

Simple groups

Definition. A group G is **simple** if its normal subgroups are only its trivial normal subgroups $\{e\}$ and G.
- For $n \neq 4$, the alternating group A_4 is simple.

QUOTIENT GROUPS

Definition. Let $(G, *)$ be a group and let K be a normal subgroup. Then define a binary operation $\diamond$ on G/K by $(g_1 K) \diamond (g_2 K) = g_1 g_2 K$.

(i) $(G/K, \diamond)$ forms the **quotient group** of G by K.
(ii) The function $\pi \colon (G, *) \to (G/K, \diamond)$ defined by $\pi(g) = gK$ is a surjective group homomorphism.
(iii) $\ker \pi = K$.

ISOMORPHISM THEOREMS

First Isomorphism Theorem

Let $\phi \colon (G, *) \to (H, \star)$ be a surjective group homomorphism. Let K be the kernel of ϕ. Then the function $\overline{\phi} \colon (G/K, \diamond) \to (H, \star)$ given by

$$\overline{\phi}(gK) = \phi(g)$$

is a well-defined group isomorphism. (In general, if ϕ is not surjective, we can simply replace H by the image $\phi(G)$).

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & H \\
& G/K \arrow[ur, "\overline{\phi}"'] &
\end{tikzcd}$$

Second Isomorphism Theorem

Let G be a group, M be a subgroup of G, and K be a normal subgroup of G. We need two propositions:
- $MK = KM$ and it is a subgroup of G.
- The function $\phi \colon M \to MK/K$ defined by $\phi(m) = mK$ is a surjective group homomorphism.
- The kernel of ϕ is $M \cap K$ (In particular it is a normal subgroup of M). Then,

$$M/(M \cap K) \simeq (MK)/K.$$

- This is a result of the First Isomorphism Theorem, as MK/K is isomorphic to $M/\ker \phi = M/M \cap K$.

Third Isomorphism Theorem

Let G be a group, and M, K be normal subgroups of G such that $K \subseteq M$. Then M/K is a normal subgroup of G/K and

$$(G/K)/(M/K) \simeq G/M.$$

- The condition $K \subseteq M$ is not very important for otherwise, we replace K by $M \cap K$ which is a normal subgroup of G contained in M.

MORE NUMBER THEORY

If $n = 1$, then we set $\Phi(1) = 1$. If $n \ge 2$, then

$$\Phi(n) = \{x \in \mathbb{Z} : 0 \le x \le n, \gcd(x, n) = 1\}.$$

- The pair $(\Phi(n), *)$ is a group, where $*$ denotes multiplication module n.

Euler's totient function
Let $\varphi(n)$ denote the number of elements in $\Phi(n)$.

Euler's Theorem
Suppose $\gcd(x, n) = 1$. Then

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Product formula
Suppose $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ is a prime factorization. Then

$$\begin{aligned}\varphi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right) \\ &= \varphi(p_1^{r_1})\varphi(p_2^{r_2})\ldots\varphi(p_k^{r_k}).\end{aligned}$$

AUTOMORPHISM GROUPS

Definition. An isomorphism $\phi \colon G \to G$ is called an **automorphism** of G. We denote the set of automorphism of G by

$$\mathrm{Aut}(G) = \{\phi \colon G \to G : \phi \text{ is an isomorphism.}\}$$

- The pair $(\mathrm{Aut}(G), \circ)$ forms a group.

Definition. Let $g \in G$, then $\phi_g : G \to G$ given by

$$\phi_g(x) = gxg^{-1}$$

is an **inner automorphism** of G. Let $\mathrm{Inn}(G) = \{\phi_g : g \in G\}$ be the set of inner automorphism.
- $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

The map $T \colon G \to \mathrm{Inn}(G)$ given by $T(g) = \phi_g$ is a surjective group homomorphism whose kernel is the *center* of the group

$$Z(G) = \{z \in G : gz = zg \text{ for all } g \in G\}.$$

By the first isomorphism theorem, we have

$$G/Z(G) \simeq \mathrm{Inn}(G).$$

SYLOW THEOREMS

Notation
Suppose p^e divides n but p^{e+1} does not divide n.
We write $p^e || n$.
Alternatively $n = p^e m$ where $p \nmid m$.

Definition. Let G be a finite group of order n, and p be a prime divisor of n. Let H be a subgroup of order p^e. Then H is called a p*-subgroup* of G. If $p^e || n$, then H is called a *Sylow* p*-subgroup* of G.

First Sylow Theorem
Let G be a group of order n, and p be a prime divisor of n.
Then G contains a *Sylow* p*-subgroup*.

Corollary
If $p^d | n$, then G contains a subgroup of order p^d.

Definition. Let P be a subgroup of G. Let $g \in G$. Then gPg^{-1} is a subgroup of G called a *conjugate* of P.
- Let P be a Sylow p-subgroup. Then a conjugate gPg^{-1} is also a Sylow p-subgroup.

Theorem
Let G be a group of order n. Let $\{P_1, P_2, \ldots, P_r\}$ be all the distinct conjugates of a Sylow p-subgroup $P = P_1$.

(i) Let Q be a p-subgroup of G. Then $Q \subseteq P_i$ for some $i \in \{1, \ldots, r\}$.
(ii) If Q is a Sylow p-subgroup of G, then $Q = P_i$ for some $i \in \{1, \ldots, r\}$.
(iii) Let r denote the number of Sylow p-subgroups of G. Then

$$r \equiv 1 \pmod{p} \text{ and}$$
$$r \text{ divides } [G : P].$$

Corollary
Let P be a Sylow p-subgroup of a finite group G. Then P is a normal subgroup if and only if P is the unique Sylow p-subgroup of G.