Group Theory notes

(1) **Definition.** A *group* is a set G together with a binary operation $\cdot : G \times G \to G$, such that
   (a) The operation $\cdot$ is associative.
   This means $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
   (b) There is an identity element in G.
   There exists $1 \in G$ so that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$.
   (c) There are inverses in G.
   For each $g \in G$ there exists $g^{-1} \in G$ so that $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

(2) **Remark.** When speaking about groups in general we often denote the binary operation by juxtaposition, writing gh for $g \cdot h$. When speaking about particular groups we may use other symbols such as $+$ or $\circ$ for the binary operation.

(3) **Examples.** We reminded ourselves of the definition of complex numbers, their addition and multiplication, and we considered the geometry behind multiplication of complex numbers (polar form).
   We gave a definition of modular (clock) arithmetic.
   Still to do. Introduce permutation groups. Introduce some matrix groups.
$(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$,
$(\mathbb{R}^+, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{C} - \{0\}, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{Q} - \{0\}, \cdot)$,
$(\{e^{2\pi i/3}, e^{4\pi i/3}, 1\}, \cdot)$, $(\{\pm 1\}, \cdot)$, $(\{\pm i, \pm 1\}, \cdot)$, $(\{e^{2\pi m i/n} \,|\, m, n \in \mathbb{Z}^+,\ 1 \le m \le n\}, \cdot)$,
$(S^1, \cdot)$ where $S^1 = \{z \in \mathbb{C} \,|\, |z| = 1\}$ is the set of unit complex numbers.
$(\mathbb{Z}_n, +)$, $(\mathbb{Z}_p - \{0\}, \cdot)$,
$(\mathrm{Perm}(\{1, 2, \ldots, n\}), \circ)$. Notation: S_n is often used to denote $(\mathrm{Perm}(\{1, 2, \ldots, n\})$,
$\mathrm{GL}(n, \mathbb{C})$, $\mathrm{GL}(n, \mathbb{R})$, $\mathrm{GL}(n, \mathbb{Q})$, $\mathrm{SL}(n, \mathbb{C})$, $\mathrm{SL}(n, \mathbb{R})$, $\mathrm{SL}(n, \mathbb{Q})$, $\mathrm{SL}(n, \mathbb{Z})$.
Orthogonal and special orthogonal groups.
Heisenberg group.
Encoding functions : $\mathbb{R} \to \mathbb{R}$ of the form $x \mapsto ax + b$ $(a \neq 0)$ by 2×2-matrices.
Isometries of the Euclidean line.

(4) **Definition.** Let $(G, \cdot)$ be a group. A subset H of G is said to be a *subgroup of* G if $1 \in H$ and if H is closed under multiplication and taking inverses. We write $H < G$ to denote that H is a subgroup of G.

(5) **Examples.**
   (a) $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$
   (b) $(\mathbb{Q}^+, \cdot) < (\mathbb{R}^+, \cdot) < (\mathbb{R} - \{0\}, \cdot) < (\mathbb{C} - \{0\}, \cdot)$
   (c) $(\{\pm 1\}, \cdot) < (\mathbb{R} - \{0\}, \cdot)$
   (d) $(\{\pm 1, \pm i\}, \cdot) < (S^1, \cdot) < (\mathbb{C} - \{0\}, \cdot)$
   (e) many more examples in class notes.

(6) **Definition.** Let G and H be groups. A *homomorphism* is a map $\varphi : G \to H$ such that

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \qquad \text{for all} \quad g_1, g_2 \in G.$$

   An *isomorphism* is a homomorphism $\varphi : G \to H$ which is a bijection.
   An isomorphism $G \to G$ is called an *automorphism of* G.

(7) **Properties.** Elementary properties of groups.
   (a) The identity element of a group is unique.
   (b) Inverses of elements in a group are unique.
   (c) Left cancellation law holds in a group. If $gx = gy$ then $x = y$.
   (d) Right cancellation law holds in a group. If $xg = yg$ then $x = y$.
   (e) A homomorphism $G \to H$ must take the identity in G to the identity in H.
   (f) A homomorphism $\varphi : G \to H$ satisfies $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.
   (g) Given $g \in G$ the *left multiplication* map $L_g : G \to G : x \mapsto gx$ is a bijection.

(8) **Cayley's Theorem.** Let G be a group. Given $g \in G$ let L_g denote the left multiplication by g map. The map

$$\Phi : G \to \mathrm{Perm}(G) \ : g \mapsto L_g$$

is an injective homomorphism. In particular, the map

$$\Phi : G \to \Phi(G) < \mathrm{Perm}(G)$$

is an isomorphism between G and the subgroup $\Phi(G)$ of $\mathrm{Perm}(G)$. In other words *every group G can be considered as a group of permutations of some set.*

(9) **Examples.** Given in class.

(10) **Cosets.** Let G be a group and $H < G$ a subgroup. Given $g \in G$ the set

$$gH \ = \ \{gx \,|\, x \in H\}$$

is called a *left coset of H in G*.

You should prove that the restriction of the left multiplication map L_g to the subset H gives a bijection

$$L_{g|_H} : H \to gH$$

(11) **Lagrange's Theorem.** Let G be a group and $H < G$ a subgroup. Then left cosets of H in G are either disjoint or equal. That is, if $g_1H \cap g_2H \neq \emptyset$, then $g_1H = g_2H$. Thus the distinct left cosets of H in G form a partition of G.

In particular, if $|G| < \infty$ and $H < G$, then $|H|$ divides $|G|$.

(12) **Transversals.** Let G be a group and $H < G$ a subgroup. A subset $T \subset G$ is called a *transversal* for H in G if it contains a single representative of every left coset of H in G. That is $T \cap gH$ is a singleton set for each distinct left coset gH of H in G.

(13) **Examples.** We saw many examples in class.
(a) $\{1, (12)\}$ is a transversal for the subgroup $\{1, (123), (132)\}$ in S_3.
(b) $\{1, (123), (132)\}$ is a transversal for the subgroup $\{1, (23)\}$ in S_3.
(c) The interval $[0, 1)$ is a transversal for $\mathbb{Z}$ in $\mathbb{R}$.
(d) There is a transversal for $\mathbb{Q}$ in $\mathbb{R}$ which is contained inside of $[0, a]$ for any positive number a.

(14) **A warm-up version of the Banach-Tarski paradox.** See later!

(15) **Order of an element.** Let G be a groups. The *order* of the element $g \in G$ is the smallest positive integer n such that $g^n = 1$. If no such positive integer exists, then g is said to have *infinite order*.

(16) **Generating sets.** Let G be a group. A subset $A \subset G$ is called a *generating set* for G if every element of G can be expressed as a product of elements of A and inverses of elements of A.

(17) **Examples.** We saw many examples in class.
(a) $\{1\}$ and $\{2, 3\}$ are generating sets for $\mathbb{Z}$.
(b) $\{(12), (123)\}$ is a generating set for S_3.
(c) $\{(12), (1 \ldots n)\}$ is a generating set for S_n.

(18) **Finitely generated groups.** A group G is said to be *finitely generated* if it has a generating set with finitely many elements.

(19) **Example.** We've seen that S_n, $\mathbb{Z}$ and $\mathbb{Z}_n$ are finitely generated.
Show that none of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are finitely generated.

(20) **Cayley graphs.** Let G be a finitely generated group, with finite generating set $A \subset G$. The *Cayley graph of G with respect to A*, denoted by $\Gamma_A(G)$, is defined as follows. The vertex set of $\Gamma_A(G)$ is take to be the set G. The edge set of $\Gamma_A(G)$ is the set $G \times A$, with an edge (g, a) connecting the vertex g to the vertex ga.

(21) **A geometric version of Cayley's theorem.** Let G be a group with finite generating set A.

We can put a distance on the Cayley graph $\Gamma_A(G)$ by requiring that each edge be either a unit interval or a circle of circumference 1 (depending on whether the endpoints of the edge are distinct or not), and then defining the distance between two points to be the length of a shortest path connecting them.

The elements of the group G move the vertices of $\Gamma_A(G)$ around by left multiplication. Since $\Gamma_A(G)$ is defined using right multiplication, and since group multiplication is associative, we see that adjacent vertices are sent to adjacent vertices by left multiplication. Thus we can see where left multiplication by elements of G sends edges of $\Gamma_A(G)$. We saw in class that left multiplication by $g \in G$ gives a bijective map of $\Gamma_A(G)$ which preserves distance. This is called an isometry of $\Gamma_A(G)$. We say that G acts on $\Gamma_A(G)$ by isometries.

(22) **Normal subgroups.** Let G be a group and $H < G$ a subgroup. We say that H is a *normal subgroup* of G if

$$gHg^{-1} \;=\; H \qquad \text{for all } g \in G$$

or equivalently if

$$gH \;=\; Hg \qquad \text{for all } g \in G.$$

We denote the fact that H is a normal subgroup of G by writing $H \lhd G$.

(23) **Quotient groups.** Let G be a group and $H \lhd G$. Then the set G/H of left cosets of H in G becomes a group under the following multiplication operation

$$(g_1H)(g_2H) \;=\; g_1g_2H$$

(24) **Kernels of homomorphisms.** Let $\varphi : G \to H$ be a homomorphism of groups. The *kernel of* φ, denoted by $ker(\varphi)$, is defined to be

$$ker(\varphi) \;=\; \{g \in G \mid \varphi(g) = 1\}$$

Prove that $ker(\varphi) \lhd G$.

Prove that $ker(\varphi)$ completely encodes the failure of φ to be injective; namely, φ is injective if and only if $ker(\varphi) = \{1\}$. You should show that $\varphi(g_1) = \varphi(g_2)$ if and only if $g_1^{-1}g_2 \in ker(\varphi)$.

(25) **Image of a homomorphism.** Let G and H be groups, and $\varphi : G \to H$ be a homomorphism. The *image of* φ is defined to be the set $\varphi(G) = \{\varphi(g) \mid g \in G\}$. It is a subgroup of H.

(26) **First isomorphism theorem.** Let $\varphi : G \to H$ be a homomorphism of groups. Then $G/ker(\varphi)$ is isomorphic to $\varphi(G)$.

(27) **Examples.** There are lots of examples around. Think of your other math classes.

(a) In linear algebra the image of a linear map $T : V \to W$ is a subspace $T(V)$ of the co-domain vector space W. The null space $null(T)$ is the kernel $ker(T)$. The first isomorphism theorem says that, as additive groups (ignore the scalar multiplication), we have an isomorphism between $V/ker(T)$ and $T(V)$. This has lots of geometric content in linear algebra. An example is the rank-nullity theorem, which states that the dimension of $T(V)$ and the dimension of $ker(T)$ add to give the dimension of V. Another example is the case of projection maps where the image and the kernel and the additivity of dimensions all make very intuitive sense.
You might like to think of the group theory version of the first isomorphism theorem as a kind of non-commutative linear algebra.

(b) Let $\varphi : \mathbb{C} - \{0\} \to S^1 : z \mapsto z/|z|$. Then $ker(\varphi)$ is the subgroup $\mathbb{R}^+$ of $\mathbb{C} - \{0\}$, and the cosets of $\mathbb{R}^+$ are the open rays from the origin of the form $e^{i\theta}\mathbb{R}^+$. The set S^1 is a transversal for the set of left cosets of $\mathbb{R}^+$ in $\mathbb{C} - \{0\}$. The first isomorphism theorem gives an isomorphism between the quotient group of left cosets $(\mathbb{C} - \{0\})/\mathbb{R}^+$ and S^1.

(c) Example 27b should enable you to write down an isomorphism between the "cylinder group" $\mathbb{R}^+ \times S^1$ and $\mathbb{C} - \{0\}$. Here the first group is the cartesian product of the multiplicative groups $\mathbb{R}^+$ and S^1. You can think of $\mathbb{C} - \{0\}$ as a circles worth of open rays $\mathbb{R}^+$. Another way to think of a circles worth of lines is as an infinite cylinder. This intuition is an important starting point in complex analysis if you are going to think about the complex exponential function and complex logarithms.

(d) $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. This is often how $\mathbb{Z}_n$ is defined in an abstract algebra course.

(e) $O(2)/SO(2)$ is isomorphic to $\mathbb{Z}_2$. Think of the determinant map.

(f) $\mathrm{Gl}(n,\mathbb{R})/\mathrm{Sl}(n,\mathbb{R})$ is isomorphic to $\mathbb{R}-\{0\}$. Think of the determinant map.
(g) $\mathrm{S}_3/\langle(123)\rangle$ is isomorphic to $\mathbb{Z}_2$.

(28) **Group actions on sets.**

(29) **Orbits, stabilizer sibgroups, and fixed sets.**

(30) **The Burnside orbit counting lemma.**

(31) **Applications of the Burnside lemma.**

(32) **Isometries of $\mathbb{R}$.**

(33) **Infinite dihedral group.**

(34) **Isometries of $\mathbb{R}^2$.**

(35) **Dihedral groups.**

(36) **Frieze pattern groups.**

(37) **Wallpaper pattern groups.**

(38) **Isometries of $\mathbb{R}^3$.**

(39) **Isometries of regular solids.**

(40) **Investigating the group $\mathrm{SO}(3)$.**

(41) **Free groups.**

(42) **Free subgroups of matrix groups.**