I. Introduction

Here is the basic information about the course.

Book) Artin's Algebra, 2nd Edition

Office Hours/Homework Dates

II. Group Theory

II.1. Basic Definitions

What are we studying in this course? Well, we study **groups**.

Definition II.1.1

A **group** is a set S equipped with a "binary operation":

$$\cdot : S \times S \to S$$
$$(s,t) \mapsto s \cdot t$$

which satisfies the following axioms:

Associativity) $s(tu) = (st)u$

Identity) There is some element e such that $s \cdot e = e \cdot s$ for all $s \in S$.

Inverses) For every $s \in S$ there is some $t \in S$ such that $st = e = ts$.

We sometimes denote such a group by the triple $(S, \cdot, e)$. One should not think about it like this.

Groups arise as *symmetries* of objects in nearly all areas of mathematics. This allows them to be broadly applied and to solve a variety of problems. Furthermore, we understand groups very very very well, and this allows us to transform problems that are challenging in other areas into problems in group theory which are perhaps less challenging.

Example II.1.1

A classic example of a symmetry group is the symmetries of a *set*, aka for a set S we can consider the set $\mathrm{Aut}(S)$ of invertible functions $S \to S$ with the operation of function composition.

This is a great example to remember for thinking of groups as symmetries.

Remark II.1.1

Some results and ideas in this course are generalized in a subject called category theory. This starts exactly... now! Do not worry if you do not know category theory. However, some remarks will be left for those that do, as well as an appendix on the subject **??**.

Category Theory formalizes the idea of symmetries of an object being a group. Namely, for an object X lying in a category $\mathscr{C}$, there is a group $\mathrm{Aut}_{\mathscr{C}}(X)$ of invertible morphisms $X \to X$ in $\mathscr{C}$.

We now move on to some basic examples and results to guide our thinking about the subject.

Example II.1.2

Lets quickly give some examples of groups to see how amazing they really are.

Symbol	Set	Operation
$\mathbb{Z}$	$\mathbb{Z}$	$+$
$\mathbb{Q}^\times$	$\mathbb{Q} \setminus \{0\}$	$\times$
$\mathrm{SL}_3(\mathbb{Z})$	3×3 matrices with det one	Matrix Mult.
$\mathrm{SL}_3(\mathbb{Z}/10\mathbb{Z})$	3×3 matrices with det one and entries in $\mathbb{Z}/10\mathbb{Z}$	Matrix Mult.
$\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$	2×2 matrices with nonzero det and entries in $\mathbb{Z}/1\mathbb{Z}$	Matrix Mult.
S_n	Permutations of $\{1, \ldots, n\}$	Composition
$C_n = \mathbb{Z}/n\mathbb{Z}$	$\{1, \ldots, n\}$ Addition modulo n.	

The group $\mathbb{Z}/n\mathbb{Z}$ is called the cyclic group of order n and is extremely important.

Interesting Note: $\mathbb{Z}/n\mathbb{Z}$ is "generated" by 1. This means that any element of $\mathbb{Z}/n\mathbb{Z}$ may be obtained by repeatedly multiplying 1 by itself.

Proposition II.1.1

Here is a list of fundamental and basic results about about groups:

- The identity element is unique. If e, e' are both identities, $e' = ee' = e$.
- The inverse of a given element $s \in S$ is unique. We call this inverse s^{-1}. Suppose $s^{-1}s = e = st$ then:
$$s^{-1} = s^{-1}e = s^{-1}(st) = (s^{-1}s)t = et = t$$
Great!
- When multiplying many elements, there is no need to write parentheses. I.e. $s_1 s_2 \cdots s_n$ (for $s_i \in S$) always evaluates to the same element of S regardless of how it is grouped.

One might think that they should understand groups by going through all of the possible sizes one by one and classifying those groups. This is awful and a terrible idea. We do it anyway to show you that it works for very small groups:

Size 1) C_1.
Size 2) C_2.
Size 3) C_3.
Size 4) C_4 and $C_2 \times C_2$ (see Definition II.1.2).
Size 5) C_5.
Size 6) S_3, C_6.
Size 7) C_7.
Size 8) Ugly.

Definition II.1.2

Given two groups G, H with respective operations $\cdot, \star$ we have that $G \times H$ is a group with the operation

$$(\cdot, \star) : (G \times H) \times (G \times H) \to G \times H$$
$$((g_1, h_1), (g_2, h_2)) \mapsto (g_1 \cdot g_2, h_1 \star h_2).$$

To study groups well we should define extra structure to think about them.

Definition II.1.3

A subgroup of a group $(G, \cdot, e)$ is a subset H of G which contains e such that $(H, \cdot, e)$ is also a group.

An equivalent definition is that H is a subet of G containing e such that:

- If $s, t \in H$ then $st \in H$.
- If $s \in H$ then $s^{-1} \in H$.

Example II.1.3

Subgroups of $\mathbb{Z}$ under addition are all $n\mathbb{Z}$ with n some arbitrary non-negative integer.

Proof. Let H be a subgroup of $\mathbb{Z}$. By definition, any subgroup contains zero. $\{0\} = 0\mathbb{Z}$ is a subgroup.

Now $H \neq \{0\}$, so it contains some nonzero element, and so it must contain some positive element because inverses correspond to negation. We then may take the smallest positive element $n \in H$.

By repeated addition, $n\mathbb{Z} \subseteq H$, so we must show that $H \subseteq n\mathbb{Z}$. To show this, let $x \in H$. By the division algorithm, $x = nq + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < n$. But then $r = x - nq \in H$, so by minimality of n, we have that $r = 0$ and $x = nq$.

Now we prove one of the most crucial results about finite groups right off the definition. To do we introduce a new concept, a "coset" and these cosets will partition our set.

Definition II.1.4

Given a group G, a subgroup H of G, and an element $g \in G$, the set $gH = \{gh \mid h \in H\}$ is called a coset of H or of g.

Theorem II.1.2 (Lagrange's Theorem)

If G is a finite group and H is a subgroup of G, then $|H|$ (the size of H) divides $|G|$. Notably the converse is not always true.

Spoecifically we have that $|G| = |H| \cdot [G : H]$, where $[G : H]$ is the number of different cosets of H in G

Proof. We do this by showing that the cosets partition G into equal pieces. Equivalently, this defines an equivalece relation on G ($g \sim g'$ if $gH = g'H$, or equivalently they belong to the same coset, equivalently $g'g^{-1} \in H$).

For $g \in G$, consider the coset gH. Clearly $|gH| = |H|$ since $gx = gy$ implies that $x = y$. Also $\bigcup_{g \in G} gH = G$ since $e \in H$, so $g = ge \in gH$.

We simply must show that $gH \cap g'H \neq \emptyset$ then $gH = g'H$. Let $x \in gH \cap g'H$, so $x = gh = g'h'$ for some $h, h' \in H$. Without loss of generality, it suffices to prove that $gH \subseteq g'H$, as the same method will show that $g'H \subseteq gH$.

Fix some $y \in gH$, then $y = gh_y$ for some $h_y \in H$. Then $y = gh_y = g'h'h^{-1}h_y \in g'H$.

Put another way, we can write this symbolically at the level of sets:

$$gH = ghh^{-1}H = g'h'h^{-1}H = gh'H = gH$$

Using the fact that $hH = H$ for any $h \in H$, which can be proven quickly using the fact that H is closed under the group operation and under inverses.

Therefore G is the union of disjoint subsets, each of size $|H|$, so $|H|$ divides $|G|$. Using the fact that $hH = H$ for any $h \in H$, which can be proven quickly using the fact that H is closed under the group operation and under inverses.

Therefore G is the union of disjoint subsets, each of size $|H|$, so $|H|$ divides $|G|$.

Corollary II.1.3

Every $g \in G$ satisfies $g^{|G|} = 1_G$ (that is the identity in G)

Proof. Let H be the group generated by g, that is all "powers" of g. Then $|H|$ is the smallest nonnegative integer so that $g^{|H|} = 1_G$ Because $|H|$ divides G, we may then write $g^{|G|} = g^{s|H|} = 1_G^s = 1_G$ for some integer s.

TODOS: