Book: Dummit & Foote: Abstract Algebra

Syllabus:
- Abelian groups
- Part II: ring theory
  (main focus: commutative rings, divisibility theory) + a little from Chapter 15
Part III: modules

Chapter 10

Skip Chapter 11.1 - 4 (vector spaces, assuming we have seen that)

modules over PID's

- Jordan canonical form
- Classification of finitely generated abelian groups etc.

- Multilinear algebra
- Exterior algebra
- bilinear, symmetric bilinear, quadratic, hermitian forms

- some concept of categorical language

Grading: Tests 100 pt. Oct 5 in class

100 pt. Nov 9

100 pt. Dec 12

No Final

graded point possible

100 pt. HW - assigned in class on Wed. except
Quizzes: generally Wednesdays 100 pts.
Office hours MWF 2-3 & by appointment EH 3846.

Abelian groups

A monoid is a set M together
with a binary operation \(* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}\) which is associative, and there is a unit element \(e \in \mathbb{R}\):

\[
(a \cdot b) \cdot c = a \cdot (b \cdot c)
\]

\[
a \cdot e = e \cdot a = a.
\]

If we omit the unit axiom, we get the definition of a semigroup.

Examples: \((C^\times, \cdot) = \{ z \in C \mid 0 < \|z\| < 1 \}\) is a semigroup.
$(\mathbb{N}, +) = (\mathbb{Z}, 1, 2, 3, \ldots, +)$ is a semigroup.

$(\mathbb{N}, 0, +) = (\mathbb{Z}, 0, 1, 2, 3, \ldots, +)$ is a monoid.

Set $(\{f : S \to S\}, *)$ is a monoid

All maps

$(\mathbb{N}, \cdot) = (\{1, 2, 3, \ldots\}, \cdot)$ is a monoid.

A group is a monoid $(G, *)$ together

with a unary operation $(?)^{-1} : G \to G$ and

that $a \ast a^{-1} = a^{-1} \ast a = e$. 
An operation \( * \) is commutative when

\[ a * b = b * a \]

Hence, we get the notion of commutative semigroup, commutative monoid,

\[ \text{commutative group} = \text{abelian group} \]

The operation \( * \) is sometimes denoted by \( \cdot \), the usual, the neutral element is usually denoted by \( 1 \). This is the multiplicative notation.
The operation $\ast$, especially when commutative, is often denoted by $\oplus$. Then the neutral element is usually denoted by $0$, the inverse to $a$ is usually denoted by $-a$. This is the additive notation.

Let $A$ be a group, $a \in A$. In the multiplicative notation, we write

$$a^k = \underbrace{a \cdot \ldots \cdot a}_{k \text{ times}} \quad k \in \mathbb{N}$$
\[ a^0 = 1 \]

\[ a^{-k} = (a \cdot \ldots \cdot a)^{-1} = \underbrace{(a^{-1} \cdot \ldots \cdot a^{-1})}_{k \text{ times}} \]

In the additive notation for an abelian group, we write \( ka \) instead of \( a^k \):

\[ ka = a + \ldots + a \quad \text{\( k \in \mathbb{N} \)} \]

\[ 0 \cdot a = 0 \]

\[ (-k) \cdot a = (-a) + \ldots + (-a) = -(a + \ldots + a) \]
A subgroup of a group \((G, \ast)\) is a subset \(H \subseteq G\) which is a group under the restriction of the operation \(\ast\):
\[
\forall a, b \in H \implies a \ast b \in H
\]
The neutral element \(e \in H\).
If \(a \in H\) \implies a^{-1} \in H.

Example: \((\mathbb{Z}, +)\) = all integers is an abelian group.
Proposition: If \( H_i, i \in I \) are subgroups of \( G \), then \( \bigcap_{i \in I} H_i \) is a subgroup of \( G \). □

If \( S \subseteq G \) is a subset, we can

\[
k \mathbb{Z} \subseteq \mathbb{Z} \quad \forall k \in \mathbb{Z}
\]

\[
d \mathbb{Z} \subseteq \mathbb{Z} \quad \forall m \in \mathbb{Z}
\]

is a subgroup.

Notation: \( \leq \)
peak of the smallest subgroup of \( G \) containing \( S \):

\[
\bigcap \{ H \leq G \mid H \supseteq S \}.
\]

This is called the subgroup generated by \( S \).

---

HW

1) Suppose \((M, \cdot)\) is a semigroup and there exist elements \( e_1 \) and \( e_2 \) such that

for all \( x \in M \),

\[
e \cdot x = x \quad x \cdot e = x.
\]

Prove that \((M, \cdot)\) is a monoid.
(2) Prove from the axioms that in a group $G$,
\[(a^{-1}) \ast (b^{-1}) = (b \ast a)^{-1}.\]

(3) Prove that for a group $G$ and a subset $S \subseteq G$, the subgroup generated by $S$ is the following:
\[\{x_1 \ast \ldots \ast x_n \mid x_i \in S \, \text{or} \, x_i^{-1} \in S\}\]

(we allow $n = 0$ in which case $x_1 \ast \ldots \ast x_n = e$).