Five Whole Days of Algebra

Notre Dame's Bridge Program
Harrison Gimenez & Lorenzo Riva

July 26-30, 2021

Day 1

Definition. A *group* is a set G together with a binary operation $- \cdot - : G \times G \to G$ that satisfies the following axioms:

(i) *associativity*: $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(ii) *existence of identity*: $\exists e \in G : \forall a \in G : a \cdot e = a = e \cdot a$;

(iii) *existence of inverses*: $\forall a \in G : \exists a^{-1} \in G : a \cdot a^{-1} = e = a^{-1} \cdot a$.

If, in addition, the operation also satisfies

$$\forall a, b \in G : a \cdot b = b \cdot a,$$

then we say that G is an *abelian group*.

Some general notation:

- If G is a finite group, the number of elements it has is denoted by $|G|$ and is called its *order*.
- $a^n := \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ copies of } a}$.
- $a^{-n} := (a^{-1})^n = \underbrace{a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1}}_{n \text{ copies of } a^{-1}}$.
- $a^0 := e$.

Here are a couple of examples of groups. They will be discussed more in the exercises.

1. The sets of numbers $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition.
2. The sets of non-zero numbers $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}, \mathbb{R}^\times := \mathbb{R} \setminus \{0\}, \mathbb{C}^\times := \mathbb{C} \setminus \{0\}$ under multiplication.
3. The set $\mathbb{R}_{>0} := \{r \in \mathbb{R} \mid r > 0\}$ of positive real numbers under multiplication
4. The *quaternion group*: the set
$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$
under the operation defined by
$$\forall a \in Q : (\pm 1) \cdot a = \pm a, \quad i^2 = j^2 = k^2 = i \cdot j \cdot k = -1.$$
This group gives rise to the *real quaternions* $\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, which also form a group under addition.

5. The unit circle $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ under multiplication; here $|z|$ denotes the length of z in $\mathbb{C}$, not its order.

6. If S is a set, the set of functions $f : S \to \mathbb{C}$ under the operation

$$(f \boxplus g)(s) = f(s) + g(s).$$

7. For fixed $m, n \in \mathbb{N}$, the set of $\mathbb{C}$-valued $m \times n$ matrices under addition and the set of $\mathbb{C}$-valued invertible $m \times m$ matrices under multiplication.

8. For a fixed positive integer n, the set $\mathbb{Z}/n\mathbb{Z}$ of *integers modulo n*: informally, $\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n-2, n-1\}$ and the operation is

$$a \boxplus b = \begin{cases} a+b & a+b \leq n-1 \text{ in } \mathbb{Z}, \\ a+b-n & a+b \geq n \text{ in } \mathbb{Z}. \end{cases}$$

9. The group of symmetries of an equilateral triangle. Concretely, one would have to pick an equilateral triangle $\triangle \subseteq \mathbb{R}^2$ in the plane, say centered at the origin, and take all the linear transformations $T : \mathbb{R}^2 \to \mathbb{R}^2$ of the plane that map the triangle to itself, i.e. $T(\triangle) = \triangle$; these form a group under function composition. Abstractly, it is the group

$$D_6 := \left\langle r, s \mid r^3 = s^2 = (sr)^2 = \mathrm{id} \right\rangle,$$

where the notation means "all the possible products of r and s, but when you see any one of $r^3, s^2, (sr)^2$ turn them into the identity". The term r represents a rotation by 120 degrees around the triangle's center, while s represents a reflection along an axis of the triangle. This is called the *dihedral group of order* 6.

Definition. Let $a \in G$. The *order* $|a|$ of a is the smallest positive n such that $a^n = e$, if it exists, and it is infinite otherwise.

Definition. Let $H \subseteq G$. Then H is a *subgroup* of G if

(i) $e \in H$;

(ii) $x \in H \implies x^{-1} \in H$;

(iii) $x, y \in H \implies x \cdot y \in H$.

In that case we write $H \leq G$.

Definition. Let $S \subseteq H$. Then $\langle S \rangle$ denotes the smallest subgroup (with respect to inclusion) of G containing all the elements of S; more precisely, $\langle S \rangle$ is a subgroup of G such that

(i) $S \subseteq \langle S \rangle$ as sets, and

(ii) if $H \leq G$ and $S \subseteq H$, then $\langle S \rangle \subseteq H$.

The subgroup $\langle S \rangle$ is said to be the *subgroup generated by S*. (Note that this definition contains an implicit assumption: that $\langle S \rangle$ exists. See problem 2.)

Definition. Let $H \leq G$. A *left coset of H* is a subset of G of the form $aH := \{ah \mid h \in H\}$ for some $a \in G$. The element a is called a *coset representative*. (Note that a is "a" representative; see the problems.)

Definition. Let $H \leq G$. The *index* $[G : H]$ of H in G is the number of distinct left cosets of H, if it is finite, or infinite otherwise.

Lagrange's Theorem. Let G be a finite group and let $H \leq G$. Then the order of H divides the order of G. More specifically,

$$|G| = [G : H] \cdot |H| .$$

Proof. See problem 4. □

Corollary. If $a \in G$ and G is finite, then $|a|$ divides $|G|$.

Proof. See problem 5. □

Definition. Let G, H be groups. A function $\varphi : G \to H$ is a *group homomorphism* if

$$\forall a, b \in G : f(a \cdot b) = f(a) \cdot f(b),$$

where the operation on the LHS is in G and the operation on the RHS is in H. A bijective group homomorphism is an *isomorphism*, and if an isomorphism $G \to H$ exists we write $G \cong H$.

See problem 6 for some important properties of group homomorphisms.

Definition. Let $H \leq G$ and define $aHa^{-1} := \{aba^{-1} \mid b \in H\}$. We say H is a *normal subgroup* of G (denoted $H \trianglelefteq G$) if $aHa^{-1} = H$ for all $a \in G$.

Theorem. Let $H \trianglelefteq G$. The set $G/H := \{aH \mid a \in G\}$ of left cosets of H in G is a group, called a *quotient group*, under the operation

$$(aH) \cdot (bH) := (ab)H.$$

Proof. See problem 10. □

Definition. Let S be a set. The *free group generated by* S, denoted $F(S)$, is the set of formal strings

$$F(S) := \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_k^{\varepsilon_k} \mid a_i \in S, \varepsilon_i \in \{1, -1\}, k \in \mathbb{N}\}$$

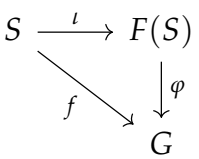
under string concatenation, with the empty word e (corresponding to $k = 0$) acting as the identity. We impose the following conditions:

(i) composition is associative;

(ii) $a \cdot a^{-1} = a^{-1} \cdot a = e$ for all $a \in S$, so that each symbol a^{-1} is an actual inverse of a.

See the exercises for some examples.

Theorem. Let $\iota : S \to F(S)$ be the inclusion map of the set S into the free group $F(S)$ (note that this is a set map, as S has no group structure). Let $f : S \to G$ be another set map into a group G. Then there exists a unique extension $\varphi : F(S) \to G$ of f, i.e. a group homomorphism satisfying $\varphi \circ \iota = f$. In short, the following diagram commutes:



Proof. See problem 13. □

Problems

1. Prove that $|G| = [G : \{e\}]$.

2. This problem will help you visualize a subgroup generated by a subset in terms of the elements of that subset.

(a) Let H, K be subgroups of G. Prove that $H \cap K$ is a subgroup of G.

(b) Generalize part (a) to arbitrary intersections: if $\{H_i \mid i \in I\}$ is a possibly infinite collection of subgroups of G, prove that $\bigcap_{i \in I} H_i$ is a subgroup of G.

(c) Let $S \subseteq G$ be a subset of G. Prove that $\langle S \rangle$ exists, i.e., produce a subgroup of G that satisfies the definition of $\langle S \rangle$ given in the notes.

(d) For $a \in G$, let $\langle a \rangle$ denote $\langle \{a\} \rangle$. Can you write down $\langle a \rangle$ explicitly?

(e) Let $S^{-1} = \{a^{-1} \in G \mid a \in S\}$. Prove that

$$\langle S \rangle = \{a_1 \cdot a_2 \cdot \cdots \cdot a_k \mid k \in \mathbb{N}, \forall i : a_i \in S \cup S^{-1}\},$$

so that $\langle S \rangle$ is given by all finite products of elements of S and inverses of elements of S. (*Hint:* For one inclusion, prove that the set on the right is a subgroup of G containing S and use the "universal property" of $\langle S \rangle$, the one given in its definition.)

3. Let $H \leq G$ and $a \in G$. Prove the following equivalences:

$$b \in aH \iff a^{-1}b \in H \iff aH = bH.$$

This means that b is also a coset representative for aH. Conclude that if $a, b \in G$ then either $aH = bH$ or $aH \cap bH = \emptyset$. (We can't have both conditions happen at the same time. Why? What would that say about aH, and hence about H?)

4. You will prove Lagrange's Theorem. In the following, let G be a finite group and $H \leq G$ a subgroup.

(a) A collection $\{S_i \mid i \in I\}$ of subsets of a set T is said to *partition* T if

(i) $T = \bigcup_{i \in I} S_i$, and

(ii) $S_i \cap S_j = \emptyset$ whenever $i \neq j$.

Use problem 2 to show that the set of cosets of H partitions G.

(b) Conclude from part (a) that $|aH| = |H|$ for all $a \in H$.

(c) Deduce the conclusion to Lagrange's Theorem.

5. Prove the corollary.

6. Let $\varphi : G \to H$ be a group homomorphism. Prove that the *kernel* $\ker \varphi := \{a \in G \mid \varphi(a) = e_H\}$ and the *image* $\operatorname{im} \varphi := \{b \in H \mid \exists a \in G : \varphi(a) = b\}$ are subgroups of their respective groups.

7. For finite H, use a size argument to show that if $aHa^{-1} \subseteq H$ (or, equivalently, $H \subseteq aHa^{-1}$) for all $a \in G$ then $H \trianglelefteq G$. How can we extend the theorem "$aHa^{-1} \subseteq H$ for all $a \in G$ iff $H \trianglelefteq G$" when H is infinite?

8. If $\varphi : G \to H$ is a group homomorphism, prove that $\ker \varphi$ is a normal subgroup of G.

9. What are the normal subgroups of an abelian group?

10. There are a couple of things to check, but the first is the most important one.

(a) Prove that the operation on the quotient group is well-defined: that is, if $a_1H = a_2H$ and $b_1H = b_2H$, then
$$(a_1H) \cdot (b_1H) = (a_2H) \cdot (b_2H).$$

(b) Prove the other group axioms. What's the identity? What are the inverses?

(c) Additionally, prove the following equivalence: H is a normal subgroup of G iff there is some other group Q and a group homomorphism $\varphi : G \to Q$ such that $H = \ker \varphi$.

11. What is the free group $F(\{a\})$ on one element? What about $F(\{a, b\})$?

12. Think about a *free abelian group* on a set S, and call it $FA(S)$. Can you write down $FA(\{a\})$ and $FA(\{a, b\})$?

13. In order to prove this theorem, first think about what the map ι does and and then about what the requisites of a group homomorphism $F(S) \to G$ are. Uniqueness might be "obvious", for once you define φ you'll see that you really made no choices. For an extra challenge, try proving that any two groups fitting in the diagram in place of $F(S)$ are isomorphic (that is, we are allowed to talk about "the" free group on S).

14. Let G be abelian. If $|a| = m, |b| = n$ are relatively prime, prove that $|ab| = mn$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$.

15. Let $H, K \leq G$. If $H \cup K \leq G$ then either $H \subseteq K$ or $K \subseteq H$. Conclude that if $G = H \cup K$ then $G = H$ or $G = K$.

16. Let G be a group of even order $2n$. Prove that there is an $a \in G$ such that $|a|$ is even. Further show that there is an *odd* number of elements of even order.

17. Recall the list of groups on pages 1-2.

1. What happens under multiplication?
4. Prove that $\mathbb{H}^\times := \mathbb{H} \setminus \{0\}$ is a group under multiplication. What important property distinguishes it from the other multiplicative groups $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$?
6. Can we replace $\mathbb{C}$ with another set? What property does that set need to have?
7. Can we replace $\mathbb{C}$ with $\mathbb{R}$ or $\mathbb{Q}$?
8. Build the group $\mathbb{Z}/n\mathbb{Z}$ as a quotient group (the notation is already pretty suggestive!) and as the kernel of a homomorphism.
9. There are groups of symmetries for all regular polygons. In fact, groups *are* representations of geometric symmetries, in a sense that will be made precise in class, maybe. Can you guess what the group of symmetries of a square and regular pentagon look like, in terms of the elements r (rotation) and s (reflection)? What are their orders?

18. Think a bit about these quotients, we will come back to them in the next lecture.

1. The quotient of $\mathbb{R}$ by $\mathbb{Z}$, where both groups have addition as their operation.
2. The quotient of $\mathbb{R}$ by $\mathbb{Q}$, where both groups have addition as their operation.

3. The quotient of the group of 2×2 invertible real matrices by the subgroup $\{I, -I\}$, with I the identity matrix.
4. The quotient of the group of 2×2 invertible real matrices by the subgroup $\{rI \mid 0 \neq r \in \mathbb{R}\}$, with I the identity matrix.
5. The quotient of the group $\mathbb{R}[x] := \{p(x) \mid p \text{ a polynomial with real coefficients}\}$ under addition by the subgroup $(x^2+1)\mathbb{R}[x] := \{(x^2+1)p(x) \mid p(x) \in \mathbb{R}[x]$.

Definition. The *symmetric group on n letters* is the set S_n of bijections $\{1,\dots,n\} \to \{1,\dots,n\}$ under function composition.

And element $\sigma \in S_n$ is usually written in cycle notation. A single cycle $(a_1, a_2, \dots, a_k)$ indicates the element $\sigma \in S_n$ defined by

$$\sigma(a) = \begin{cases} a_{i+1} & a = a_i, i = 1,\dots,k-1, \\ a_1 & a = a_k, \\ a & \text{otherwise.} \end{cases}$$

A general element σ is given by composing disjoint cycles:

$$\sigma = (a_{1,1},\dots,a_{1,k_1})(a_{2,1},\dots,a_{2,k_2})\cdots(a_{m,1},\dots,a_{m,k_m}),$$

with each $p \in \{1,\dots,n\}$ appearing exactly once among the $a_{i,j}$ unless they are fixed by σ, in which case they are omitted. As an example, the element of S_6 given by

$$\sigma : \begin{cases} 1 & \mapsto & 4 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 6 \\ 4 & \mapsto & 5 \\ 5 & \mapsto & 1 \\ 3 & \mapsto & 6 \end{cases}$$

is represented by the cycle $\sigma = (1,4,5)(3,6)$.
Composition of cycles is done right-to-left: the product $\sigma\tau \in S_n$ is the function taking $i \in \{1,\dots,n\}$ to $\tau(i) \in \{1,\dots,n\}$ and then to $\sigma(\tau(i)) \in \{1,\dots,n\}$.

Definition. Let S be a set and G a group. An *action of G on S* is a group homomorphism $G \to \mathrm{Sym}(S)$, where $\mathrm{Sym}(S)$ is the group of bijections of S (see problem 2). More concretely, it is an assignment $g \mapsto b_g$, where b_g is a bijection on S, such that

(i) $\rho_e = \mathrm{id}_S$, and

(ii) $\rho_{a\cdot b} = \rho_a \circ \rho_b$, where the circle denotes composition of functions.

This is also called a *permutation representation* and is a generalization of a *group representaton*. Sometimes we denote $\rho_a(x)$ by $a \cdot x$ to emphasize that the group G is acting via some "multiplication" on the elements of S.

Here are some examples of group actions. See problem 4.

1. The group of invertible $n \times n$ matrices acts on $\mathbb{R}^n$ via the usual matrix-times-column-vector process: $M \cdot v = M(v)$ for a matrix M and a vector $v \in \mathbb{R}^n$.

2. The dihedral group D_{2n} acts on the set of points of a regular n-gon. This can be visualized by drawing the n-gon in $\mathbb{R}^2$, at which point we can turn an element of D_{2n} into a 2×2 matrix and use the preceding example.

3. S_n acts on the set $\{1,\dots,n\}$. Indeed, $S_n = \mathrm{Sym}(\{1,\dots,n\})$!

4. The group of real numbers under addition acts on the set of functions $f : \mathbb{R} \to \mathbb{R}$ by translation: the new function $t \cdot f$ is the function given by translating f, i.e. $(t \cdot f)(x) = f(x+t)$.

5. Groups act on themselves in various ways. One is conjugation, where $g \cdot h = ghg^{-1}$. Another is left-multiplication, where $g \cdot h = gh$ (just the regular multiplication on G).

(Noether's) First Isomorphism Theorem. If $\varphi : G \to H$ is a group homomorphism with kernel $K = \ker \varphi$, then there is an isomorphism

$$f : G/K \to \operatorname{im} \varphi$$

given by $f(aK) = \varphi(a)$

Proof. See problem 5. □

Cayley's Theorem. Every finite group G is isomorphic to a subgroup of a symmetric group. The latter can be chosen to be S_n if $|G| = n$.

Proof. See problem 6. □

Definition. Let G act on the set S and let $s \in S$.

- The set $G \cdot s := \{t \in S \mid \exists g \in G : t = g \cdot s\} \subseteq S$ is called the *orbit of s under G*.
- The set $G_s := \{a \in G \mid a \cdot s = s\} \subseteq G$ is called the *stabilizer of s under G*. See problem 7.

Orbit-Stabilizer Theorem. Let G be a finite group acting on a finite set S, and let $s \in S$. Then $|G| = |G \cdot s|\,|G_s|$.

Proof. See problem 8. □

Problems

1. Are cycle decompositions unique? Find two cycles that represent the same element of S_8.

2. Prove that the composition of two bijections from a set A to itself is a bijection, that there is an identity among such bijections, and that each such bijection has an inverse. Conclude that S_n is a group.

3. These problems are meant to help you think about cycle decompositions.

(a) Find the order of a single cycle $(a_1, a_2, \ldots, a_k)$ in S_n.

(b) Find the order of the product of two disjoint cycles (you can use previous problems!) and use it to find the order of any element of S_n in terms of the order of one of its cycle decompositions. Produce an element of order 6 in S_5. Is there an element of order 9 in S_7?

(c) Let $\tau_i = (i, i+1)$ in S_n denote the *simple transpositions*. Which pairs of simple transpositions commute? Prove that $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$ for $i = 1, \ldots, n-2$.

(d) Show that each $\sigma \in S_n$ is a product of simple transpositions, i.e. that $S_n = \langle\{\tau_1, \tau_2, \ldots, \tau_{n-1}\}\rangle$. Use that to prove that $S_n = \langle\{(1,2), (1,2,\ldots,n-1,n)\}\rangle$.

4. Unless the definitions are obvious to you, you should verify that all the given examples of group actions do indeed satisfy the definition of a group action.

5. Prove that f is well-defined and that it is indeed an isomorphism.

6. This might be a tad hard. Consider the action of G on itself given by left-multiplication, so that we have a homomorphism $\rho : G \to \mathrm{Sym}(G)$. Note that $\mathrm{Sym}(G)$ is the group of *set bijections* on G, not *group isomorphisms* of G; it contains all the permutations of the elements of G, regardless of how they behave with respect to the operation on G.

(a) Prove that ρ is injective. This amounts to saying that $\rho_a = \rho_b$ implies $a = b$.

(b) Prove that an injective homomorphism has trivial kernel and that $M/\{e\} \cong M$ for any group M.

(c) Use the First Isomorphism Theorem to show that G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

(d) Find an isomorphism $\mathrm{Sym}(G) \cong S_n$.

(e) Derive the conclusion of Cayley's Theorem.

7. Prove that the stabilizer of an element of S is a subgroup of G.

8. It's easier to show that $[G : G_s] = |G \cdot s|$. Find a bijection between the set of left cosets of G_s in G and the orbit of S.

Definition. A *ring* R is a set together with two binary operations, $+$ and $\times$, satisfying the following properties:

(i) $(R, +)$ is an abelian group;

(ii) *associativity of* $\times$: $\forall a, b, c \in R : (a \times b) \times c = a \times (b \times c)$;

(iii) *distributivity of* $\times$ *over* $+$: $\forall a, b, c \in R : (a + b) \times c = a \times c + b \times c$ and $a \times (b + c) = a \times + a \times c$.

A ring is *commutative* if $\times$ is commutative.

Here are some examples of rings. See the exercises for more information.

1. The sets of numbers $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition and multiplication.
2. The set $\mathbb{R}_{>0}$ of positive real numbers with "addition" given by real multiplication and "multiplication" given by $a \boxtimes b = e^{\ln(a)\ln(b)}$.
3. The set $M_n(R)$ of $n \times n$ matrices under matrix addition and matrix multiplication, where R is one of the number rings in example 1. There are heaps of rings containing just some matrices inside $M_n(R)$, e.g. all diagonal matrices, all upper-diagonal matrices, etc., and those are in fact *subgrings* of $M_n(R)$, as we will see later.
4. The *(real) quaternions* $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$, where addition is the usual addition in $\mathbb{R}^4$ and multiplication is generated by the relation $i^2 = j^2 = k^2 = i \times j \times k = -1$.
5. For $n > 0$, the abelian group $\mathbb{Z}/n\mathbb{Z}$ with multiplication taken modulo n.
6. Let G be a group (written multiplicatively). The *group ring* $\mathbb{Z}[G]$ is given by the set of formal finite linear combinations of elements of G,

$$\mathbb{Z}[G] = \left\{ \sum_{i=1}^{m} n_i g_i \,\middle|\, n_i \in \mathbb{Z}, g_i \in G, m \in \mathbb{N} \right\},$$

   equipped with the distributive product induced by the multiplication in G. For example,

$$(n_1 g_1 + n_2 g_2) \times (n_3 g_3 + n_4 g_4) = (n_1 n_3) g_1 g_3 + (n_1 n_4) g_1 g_4 + (n_2 n_3) g_2 g_3 + (n_2 n_4) g_2 g_4.$$

7. If S is a set and R a ring, the set of functions $f : S \to R$ with pointwise addition and multiplication, i.e.

$$(f \boxplus g)(s) = f(s) + g(s), \quad (f \boxtimes g)(s) = f(s) \times g(s).$$

8. If R is a ring, the set $R[x]$ of single-variable polynomials under polynomial addition and multiplication is a ring, and so are $R[x, y] := (R[x])[y]$ (polynomials in two variables), $R[x, y, z] := (R[x, y])[z]$ (polynomials in three variables), etc.
9. Let d be a squarefree integer (if $p \mid d$ then $p^2 \nmid d$) and let

$$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

   This is a ring (in fact, a subring of $\mathbb{C}$) under addition and multiplication of complex numbers.

Definition. A ring R is *unital* if there exists $1 \in R$ with $1 \times a = a = a \times 1$ for all $a \in R$.

Definition. A unital ring is called a *division ring* if for every non-zero $x \in R$ there exists $x^{-1} \in R$ such that $x^{-1} \times x = x \times x^{-1} = 1$.

Definition. A *field* is a commutative division ring with $1 \neq 0$.

Proposition. Let R be a ring.

(i) For every $a \in R$, $a \times 0 = 0 = 0 \times a$.

(ii) If R has a multiplicative identity 1, then for all $a \in R$ we have that $-a$ (the additive inverse of a) equals $(-1) \times a$, where -1 is the additive inverse of 1.

Proof. See problem 2. □

Definition. A non-zero element $a \in R$ is a *zero divisor* if there is a non-zero $b \in R$ such that $a \times b = 0$ or $b \times a = 0$. A commutative unital ring with $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

Definition. Let R be a unital ring with $1 \neq 0$. An element $u \in R$ is a *unit* if there is some $v \in R$ such that $u \times v = v \times u = 1$.

Definition. A *subring* of a ring R is a an additive subgroup of $(R, +)$ that is closed under multiplication.

Note: to show that S is a subrgoup of R, it is enough to show that $S \neq \emptyset$ and that S is closed under subtraction and multiplication.

Definition. A *ring homomorphism* $\varphi : R \to S$ between two rings R, S is a function of the underlying sets satisfying $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$. A bijective ring homomorphism is called an *isomorphism*, and we denote by $R \cong S$ the existence of an isomorphism $R \to S$.

Definition. Let $I \subseteq R$ be a subset of R. For $r \in R$, define $rI := \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$. We say that I is an *ideal* of R if I is a subring of R and $rI, Ir \subseteq I$ for all $r \in R$. Equivalently, I is an ideal if it is closed under subtraction and it is invariant under left and right multiplication.

Here are some examples of ideals.

1. The subset $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal of $\mathbb{Z}$.

2. In general, the subsets $rI, Ir \subseteq R$ are ideals, called (left and right, respectively) *principal ideals*. When R is commutative, we denote $rI = Ir$ by (r).

3. The zero ideal (0) and the whole ring R are called *trivial ideals*. An ideal that is a proper subset of R is called a *proper ideal*.

4. Let S be a set, T the ring of functions $f : S \to R$ (as in example 7), and fix $s \in S$. The set

$$\{f \in T \mid f(s) = 0\} \subseteq T$$

is an ideal of T.

5. Let $M_n(R)$ be the ring of $n \times n$ matrices valued in a ring R and let I be an ideal of R. The subset of $M_n(R)$ consisting of matrices whose coefficients all lie in I is an ideal of $M_n(R)$.

Theorem. Let I an ideal of R. The set $R/I := \{r + I \mid r \in R\}$, where $r + I = \{r + a \mid a \in I\}$, is a ring under the operations

$$(r + I) \boxplus (s + I) = (r + s) + I, \quad (r + I) \boxtimes (s + I) = (r \times s) + I$$

Conversely, if I is a subset of R such that R/I is a ring (under the operations above) then I is an ideal of R.

Proof. See problem 7. □

Theorem. I is an ideal of R iff it is the kernel of some ring homomorphism $\varphi : R \to S$.

Proof. See problem 8. □

First Isomorphism Theorem. Let $\varphi : R \to S$ be a ring homomorphism with kernel $I = \ker \varphi$. Then the homomorphism $R/I \to \operatorname{im} \varphi$ given by $r + I \mapsto \varphi(r)$ is an isomorphism.

Proof. See problem 9. □

Fourth Isomorphism Theorem. Let I be an ideal of R. The set map

$$\left\{ \begin{matrix} \text{ideals of } R \\ \text{containing } I \end{matrix} \right\} \to \left\{ \begin{matrix} \text{ideals} \\ \text{of } R/I \end{matrix} \right\}$$

given by $J \mapsto J/I$ is an inclusion-preserving bijection.

Proof. See problem 10. □

Proposition. Let R be a unital ring with $1 \neq 0$.

(i) An ideal I of R is equal to R iff it contains a unit.

(ii) Assume R is commutative. Then R is a field iff its only ideals are trivial (the zero ideal and the whole ring).

Proof. See problem 12. □

Definition. Let R be unital and commutative, with $1 \neq 0$, and let I be an ideal of R. I is said to be

- *prime* if $I \neq R$ and $a \times b \in I$ implies $a \in I$ or $b \in I$, and
- *maximal* if it is maximal with respect to inclusion of ideals, i.e. $I \subseteq J$ implies $J = I$ or $J = R$ for all ideals J.

Maximal ideals are defined in the same way for rings that are not necessarily commutative or unital.

Theorem. Let I be an ideal of R (commutative, unital, $1 \neq 0$). Then I is prime iff R/I is an integral domain, and I is maximal iff R/I is a field.

Proof. See problem 13. □

Corollary. Maximal ideals are prime.

Problems

1. Recall the list of rings on page 9.

(a) Prove that $(\mathbb{R}_{>0}, \times, e^{\ln(-)\ln(-)})$, the ring in example 2, is actually a ring. What do you have to check, and what can be easily inferred from the algebraic properties of the standard real numbers?

(b) In the definition of $\mathbb{Z}[G]$ we can replace $\mathbb{Z}$ with any ring R. Prove that the resulting group ring $R[G]$ is, in fact, a ring.

(c) Find the unit in the rings described in examples 2, 4, 6, 7.

(d) Which of the listed examples are division rings?

(e) Which are fields?

(f) Which have zero divisors?

(g) Describe some units of the rings in examples 6 and 7.

2. Prove the proposition. Hint: (i) can be used to prove (ii).

3. Prove that all fields are integral domains.

4. Let $\varphi : R \to S$. Prove that $\ker \varphi := \{a \in R \mid \varphi(a) = 0_S\}$ and $\operatorname{im} \varphi := \{b \in S \mid \exists a \in R : \varphi(a) = b\}$ are subrings of R and S, respectively.

5. There is a notion of *left ideal* (and *right ideal* as well), where we only require $rI \subseteq I$ (respectively, $Ir \subseteq I$) in the definition of an ideal. Here is a fun exercise.

(a) Let $M_2(\mathbb{Q})$ denote the ring of 2×2 matrices with coefficients in $\mathbb{Q}$. Show that

$$P := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \,\middle|\, a, b \in \mathbb{Q} \right\}$$

is a left ideal of $M_2(\mathbb{Q})$ but not a right ideal.

(b) Let I be a non-zero ideal (both left and right!) of $M_2(\mathbb{Q})$. Show that

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I.$$

(c) Show that $e_{12}, e_{21}, e_{22} \in I$, where e_{ij} has a 1 in the (i, j) slot and zeros everywhere else.

(d) Show that *any* $A \in M_2(\mathbb{Q})$ is also in I, and conclude that I is not proper.

The conclusion is that $M_2(\mathbb{Q})$ has no non-zero proper (two-sided) ideals; of course, this can be generalized to $M_n(k)$ for any field k. The matrix rings over a field share this property with fields themselves, as you saw in the lecture, but they are not fields themselves because there are some non-zero non-invertible matrices.

6. (I'm referring to example 4 in the list of ideals.) There is a way to phrase $\{f \in T \mid f(s) = 0\}$ as a kernel of some ring homomorphism, which would give a second proof of the fact that it is an ideal. Find this homomorphism.

7. Much like in the group case, you should first prove that $\boxplus$ and $\boxtimes$ are well-defined. Once that is done, the ring axioms will follow from those of R.

8. Prove the theorem. Sorry, any hints would give this away immediately.

9. Given that we already have a first isomorphism theorem for groups, this should be easy.

10. For surjectivity, let $K \subseteq R/I$ be an ideal and consider the set $J = \bigcup_{L \in K} L$. Prove that J is an ideal of R containing I and that $J/I = K$.

11. Prove the second and third isomorphism theorems:

- if I is an ideal of R and S a subring of R, then $(S + I)/I \cong S/(S \cap I)$;
- if I, J are ideals of R and $I \subseteq J$, then $(R/I)/(J/I) \cong R/J$.

Note that there are some implicit assumptions in the above statements: that $S + I$ is a ring, that $S \cap I$ is an ideal of $S + I$, and so on. It is up to you to decide whether you feel comfortable enough with those assumptions to declare them obvious. If you don't find them obvious, I suggest you take a crack at them before getting to the main claim in each theorem.

12. You can use (i) to prove (ii).

13. Use the fourth isomorphism theorem to analyze the ideals of R/I and recall the previous proposition.

14. An element $r \in R$ is *nilpotent* if $r^n = 0$ for some $n \in \mathbb{N}$. Show that if r is nilpotent then $1 + r$ is a unit in R.

15. If r is nilpotent in R, prove that $1 - rx$ is a unit in $R[x]$.

16. Let $a \in R$ and let $C(a) = \{r \in R \mid ra = ar\}$, the *centralizer* of a.

(a) Prove that $C(a)$ is a subring of R.

(b) Prove that the set of subrings of R is closed under arbitrary intersections.

(c) Let $Z(R) := \{r \in R \mid \forall a \in R : ra = ar\}$ and show that

$$Z(R) = \bigcap_{a \in R} C(a).$$

Conclude that $Z(R)$ is a subring of R.

Day 4

In the following, all rings are commutative and unital. R always denotes one such ring.

Definition. A *norm* N on an integral domain R is a function $N : R \to \mathbb{N}$ such that $N(0) = 0$. Then R is said to be an *Euclidean domain* if it has a norm N such that for any $a, b \in R$ with $b \neq 0$ there are $q, r \in R$ with

$$a = qb + r \quad \text{and } r = 0 \text{ or } N(r) < N(b).$$

Here are some examples.

1. Any field is a Euclidean domain: since $a = (a/b)b + 0$ it is enough to set $N(a) = 0$ for all a.
2. The integers with $N(a) = |a|$ form a Euclidean domain, with the division being ordinary division with remainder.
3. The polynomial ring $\mathbb{R}[x]$ is a Euclidean domain with $N(p) = \deg p$. The division is polynomial long division (see problem 1).

Definition. A *principal ideal domain* (henceforth a *PID*) is an integral domain whose every ideal is principal.

Theorem. Every Euclidean domain is a PID.

Proof. See problem 2. □

This theorem already gives us a bunch of examples of PIDs. Some PIDs are of the form $\mathbb{Z}[\theta]$ for some $\theta \in \mathbb{C}$, but proving that they are in fact PIDs is tedious. Here is a non-example of both a PID and a Euclidean domain.

Proposition. The ring $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean domain.

Proof. See problem 3. □

Definition. We say that *a divides b*, written $a \mid b$, if $b = ac$ for some $c \in R$.

Definition. Let R be an integral domain.

- Suppose $r \in R$ is not zero or a unit. Then r is *irreducible* if $r = ab$ implies $a \in R^\times$ or $b \in R^\times$. That is, the only factors of r are itself and products of itself with units.
- A non-zero $p \in R$ is said to be *prime* if the ideal (p) is prime. In other words, p is prime if it is not a unit and $p \mid ab$ implies $p \mid a$ or $p \mid b$.
- Two elements $a, b \in R$ are *associates* if there is a unit u such that $a = ub$.

Proposition. In a PID, a non-zero element is prime iff it is irreducible.

Proof. See problem 8. □

Definition. A *unique factorization domain* (henceforth a *UFD*) is an integral domain R in which every r that is neither 0 nor a unit has the following two properties:

(i) $r = p_1 p_2 \cdots p_k$ for some irreducibles $p_i \in R$, and

(ii) the above decomposition is unique up to associates: if $r = q_1 q_2 \cdots q_l$, then $k = l$ and we can rearrange the factors so that p_i and q_i are associates for each i.

This theorem is not worth proving here, but rest assured that you see a proof of it in the Fall.

Theorem. Every PID is a UFD.

We thus already have many examples of UFDs. Also:

1. Applying the theorem to $\mathbb{Z}$ and then restricting to $\mathbb{N}$ gives us the *Fundamental Theorem of Arithmetic*: every $n \in \mathbb{N}$ is either 0, 1, or a unique product of prime numbers.
2. The polynomial ring $R[x]$ whenever R is a UFD. By induction, so are $R[x_1, \ldots, x_n]$ for any n.
3. A non-example (related to the problems) is $\mathbb{Z}[\sqrt{-5}]$. In fact, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Finally, another theorem not worth proving but useful to know. (If you want to take a crack at it, let us know if you want hints.)

Theorem. In a UFD, a non-zero element is prime iff it is irreducible.

Here is a handy chain of inclusions:

$$\text{fields} \subset \text{Euclidean dom.s} \subset \text{PIDs} \subset \text{UFDs} \subset \text{IDs} \subset \text{comm. rings} \subset \text{rings}.$$

These inclusions are all strict: $\mathbb{Z}$ is a Euclidean domain but not a field, $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a PID but not a Euclidean domain, $\mathbb{Z}[x]$ is a UFD but not a PID, $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not a UFD, $C^0(\mathbb{R}, \mathbb{R})$ (continuous functions from $\mathbb{R}$ to $\mathbb{R}$) is a commutative ring but not an integral domain, and $M_2(\mathbb{Z})$ is a non-commutative ring.

Problems

1. Prove that $k[x]$, for k a field, is a Euclidean domain. This amounts to proving that long polynomial division works formally.

(a) Pick $f, g \in k[x]$; we claim that $f = qg + r$ for $q, r \in k[x]$ with $r = 0$ or $\deg r < \deg g$. To prove this claim, we will proceed by induction on the degree of f. Show that if $\deg f = 0$ the claim holds.

(b) Assume by induction that the claim holds for all h with $\deg h \leq n$ and assume $\deg f = n + 1$. Show that the claim holds when $\deg g > n + 1$.

(c) Now assume $\deg g \leq n + 1$. Find a monomial m such that $\deg(f - mg) \leq n$. Apply the induction hypothesis and conclude the proof of the claim.

(d) Note that k is a field. Why do we need this assumption? What can't we do in $R[x]$, for R a ring that is not a field?

2. Hint: pick an ideal I and find $a \in I$ such that $N(a)$ is minimal (how do we know such an a exists?), then show that $I = (a)$.

3. Hint: prove that the ideal $(2, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ is not principal, so by the theorem we have that $\mathbb{Z}[\sqrt{-5}]$ is not a PID and hence not a Euclidean domain. Other hint: prove that 3 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$ and then use the proposition that says that irreducibles are primes in a PID.

4. Let R be an integral domain. If $(d) = (d')$ as ideals of R, then $d = ud'$ for some unit $u \in R$.

5. Prove that every non-zero prime ideal in a PID is maximal.

6. Prove that if R is a PID and I is a prime ideal of R, then R/I is also a PID.

7. Prove that any two elements a, b of a PID have a *least common multiple*: an element c such that $a \mid c$ and $b \mid c$, and if $a \mid d$ and $b \mid d$ then $d \mid c$.

8. Prove first that primes are irreducible in any integral domain. Then use the PID condition to show that an irreducible element is prime. You might want to use problem 5 (though this is possible to do without it).

9. Prove that $\mathbb{Z}[x]$ is a UFD but not a PID.

10. In this problem you will construct the *localization of a ring R with respect to a subset D*, which, informally, is another ring containing R in which the elements of D are invertible. Let R be a commutative ring and $D \subseteq R$ a subset that does not contain zero or any zero divisors and is closed under multiplication.

(a) Let $F = R \times D$ and define a binary relation $\sim$ on F by $(r, d) \sim (s, e)$ if $re = sd$ in R. Prove that $\sim$ is an equivalence relation.

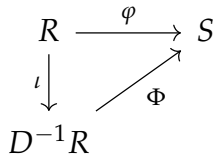
(b) Let $Q = F/\sim$ and denote $[(r, d)] \in Q$ by r/d. Let

$$\frac{r}{d} \boxplus \frac{s}{e} := \frac{re + ds}{de}, \quad \frac{r}{d} \boxtimes \frac{s}{e} := \frac{rs}{de}$$

be two binary operations on Q. Prove that $\boxplus$ and $\boxtimes$ are well-defined and then prove that $(Q, \boxplus, \boxtimes)$ is a commutative unital ring. This ring Q is denoted by $D^{-1}R$.

(c) Fix $d \in D$. Prove that the map $\iota : R \to D^{-1}R$ defined by $r \mapsto rd/d$ is an injective ring homomorphism.

(d) Let $\varphi : R \to S$ be an injective ring homomorphism into a commutative unital ring such that $\varphi(D) \subseteq S^\times$, i.e. each element of D is sent to a unit. Prove that there exists a unique injective ring homomorphism $\Phi : D^{-1}R \to S$ such that $\Phi \circ \iota = \varphi$, so that the following diagram commutes:



(e) Prove that $D^{-1}R$ is unique up to isomorphism among the commutative unital rings with an embedded copy of R in which all elements of D are units. That is, if Q' is a commutative unital ring and $\iota' : R \to Q'$ is an injective ring homomorphism that sends D to a set of units, then $D^{-1}R \cong Q'$ (in fact, there is only one such isomorphism!).

(f) What is $D^{-1}R$ isomorphic to in the case $R = \mathbb{Z}, D = \mathbb{Z} \setminus \{0\}$? What about $R = \mathbb{Z}[x], D = \mathbb{Z}[x] \setminus \{0\}$

11. Prove that if R is a PID and D is a multiplicatively closed subset of R, then $D^{-1}R$ is a PID.

Today, all rings are unital. (The ones that are usually unitless gain a temporary unit that they can use until 11:59 PM, and they are expected to clean it before returning it.)

Definition. A *left R-module* M is a set with

(i) a binary operation that makes it into an abelian group, and

(ii) a left action of R, so a function $R \times M \to M$ (denoted by $(r, m) \mapsto rm$) that is left associative and distributive with respect to the addition on R and M, i.e. for all $r, s \in R, m, n \in M$ we have

- $(rs)m = r(sm)$ (left associativity),
- $r(m + n) = rm + rn$ (distributivity in M),
- $(r + s)m = rm + sm$ (distributivity in R), and
- $1_R m = m$.

Definition. A *module homomorphism* between two R-modules M and N is an abelian group homomorphism $\varphi : M \to N$ such that $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$. The set of such homomorphism is denoted by $\mathrm{Hom}_R(M, N)$. A bijective module homomorphism is a *module isomorphism*.

Here are some examples of modules.

1. Any ring R is an R-module, with the action given by left multiplication.
2. Abelian groups of matrices with entries in any R-module M are R-modules: the action is given by scalar multiplication, namely $r(a_{ij}) = (ra_{ij})$ for any matrix (a_{ij}) and $a_{ij} \in M$. Any ring S of matrices over a ring R (i.e. S is also closed under matrix multiplication) is again an R-module, so in particular it is an associative algebra over R.
3. Vector spaces are modules over a field k.
4. Abelian groups G are $\mathbb{Z}$-modules. The action of $k \in \mathbb{Z}$ on $a \in G$ is given by $ka = a + a + \cdots + a$, the sum of k copies of a.
5. The set $\mathrm{Hom}_R(M, N)$ is actually an R-module. Addition and the R-action are given by the pointwise addition and action on N:

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m), \quad (r\varphi)(m) = r\varphi(m)$$

   for all $\varphi, \psi \in \mathrm{Hom}_R(M, N)$, $r \in R$, $m \in M$.
6. The module $\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M)$ is special in that it is also a ring, where the multiplication is given by function composition: $\varphi \times \psi = \varphi \circ \psi$. In fact, it is an associative algebra over R.
7. The group ring $R[G]$ that we saw some days ago is an R-module, with action given by left multiplication by elements of R.
8. The abelian group of functions $C(S, M)$ from a set S to an R-module M is again an R-module.
9. The ring $R[x_1, \ldots, x_n]$ of polynomials in any number of variables over R is an R-module.

10. Here is a fun module that you'll see in the future. Let $T : \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation. We can consider the polynomial ring $\mathbb{R}[T]$ of polynomials in T with real coefficients, where T^k is to be interpreted as $T \circ \cdots \circ T$, the composition of k factors of T. Then the vector space ($\mathbb{R}$-module) $\mathbb{R}^n$ has the structure of an $\mathbb{R}[T]$-module: the action of $p(T) = r_k T^k + \cdots + r_1 T + r_0 \in \mathbb{R}[T]$ on $v \in \mathbb{R}^n$ is given by

$$p(T)v = r_k T^k(v) + \cdots + r_1 T(v) + r_0 v \in \mathbb{R}^n.$$

Definition. A *submodule* N of an R-module M is a subgroup of M that is also closed under the R-action: $rn \in N$ for all $r \in R$, $n \in N$.

Proposition. Let N be a submodule of the R-module M. The quotient M/N of abelian groups is an R-module whose action is given by $r(a + N) = ra + N$.

Proof. See problem 1. □

Note that we can quotient out by any submodule, unlike for general groups and rings. This is a consequence of the underlying abelian structure.

First Isomorphism Theorem. If $\varphi : M \to N$ is a morphism of R-modules with kernel $I = \ker \varphi$, then $M/I \cong \operatorname{im} \varphi$.

Proof. See problem 2. □

Fourth Isomorphism Theorem. Let N be a submodule of the R-module M. The set map

$$\left\{\begin{matrix}\text{submodules of } M \\ \text{containing } N\end{matrix}\right\} \to \left\{\begin{matrix}\text{submodules} \\ \text{of } M/N\end{matrix}\right\}$$

given by $J \mapsto J/N$ is an inclusion-preserving bijection.

Proof. See problem 3. □

Definition. Here are some constructions with modules. In what follows M will be an R-module, N_i will be a submodule of M for each i in some indexing set I, and A will be a subset of M. Moreover, M_j will be an R-module for each j in some indexing set J; we don't require any relationship between the M_j's.

1. The *sum* $\sum_{i \in I} N_i$ is the submodule of M with underlying set

$$\sum_{i \in I} N_i := \{a_{i_1} + a_{i_2} + \cdots + a_{i_k} \mid a_{i_j} \in N_{i_j}, k \in \mathbb{N}\}.$$

2. By RA we mean the submodule of M with underlying set

$$RA := \{r_1 a_1 + \cdots + r_k a_k \mid r_i \in R, a_i \in A, k \in \mathbb{N}\}.$$

   A submodule N of M is said to be *finitely generated* if $N = RA$ for some finite subset A.

3. The *direct product of modules*, denoted by $\prod_{j \in J} M_j$, is the R-module

$$\prod_{j \in J} M_j := \{(a_j)_{j \in J} \mid a_j \in M_j\}$$

of J-tuples under componentwise addition and scalar multiplication:

$$(a_j)_{j\in J} + (b_j)_{j\in J} = (a_j + b_j)_{j\in J}, \quad r(a_j)_{j\in J} = (ra_j)_{j\in J}.$$

If J is finite we write $M_{j_1} \times \cdots \times M_{j_l}$. Formally, $\prod_{j\in J} M_j$ is the set of set functions $f : J \to \bigcup_{j\in J} M_j$ such that $f(j) \in M_j$ for all $j \in J$, equipped with pointwise addition and scalar multiplication.

4. The *direct sum of modules*, denoted by $\bigoplus j \in JM_j$, is the submodule of $\prod_{j\in J} M_j$ consisting of all J-tuples in which only finitely many entries are non-zero. M is said to be *free* if $M \cong \bigoplus_{i\in J} R$.

Proposition. Let $N_1, \ldots, N_k$ be submodules of an R-module M. The following are equivalent:

1. The map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ given by $(n_1, \ldots, n_k) \mapsto n_1 + \cdots n_k$ is an isomorphism.
2. $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for every $1 \leq j \leq k$.
3. Every $x \in N_1 + \cdots + N_k$ can be written *uniquely* as $x = n_1 + \cdots + n_k$ with $n_i \in N_i$.

Proof. See problem 5. □

Problems

1. Prove that the R-action described in the proposition is well-defined and show that M/N is an R-module.

2. Prove that $\ker \varphi$ and $\operatorname{im} \varphi$ are submodules of M and N, respectively, then prove the theorem.

3. Ask Harrison for hints if you need any.

4. Prove that if J is finite then $\bigoplus_{j\in J} M_j = \prod_{i\in J} M_j$.

5. I think 1 $\iff$ 3 and 2 $\iff$ 3 are easier to prove than 1 $\iff$ 2.

6. Show that for $R = \mathbb{Z}[\sqrt{-5}]$, the module $R(\{2, 1 + \sqrt{-5}\})$ is a submodule of R that is not free, i.e. not isomorphic to R.

7. This is a free problem. Ask about anything you want, from this or previous homework sets, from the lectures, from your own readings, etc. You can also ask to solve this problem if you want to talk about other classes, living in South Bend, seminars, cooking, chess strategies, where to play ping pong, video games, etc.