Week 0: The definition of a ring and examples

Let R be a ring with identity.

Practice Problems

1. Let X be a nonempty set. Define addition and multiplication operations on the power set $\mathcal{P}(X)$ by $A + B = (A \setminus B) \cup (B \setminus A)$ and $A \times B = A \cap B$. Show that $\mathcal{P}(X)$ is a commutative ring with identity.
2. Show that $Z(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$ is a subring of R containing the identity. Show that if R is a division ring then $Z(R)$ is a field.
3. Let $\alpha \in \mathbb{C}$ be such that $\alpha^2 \in \mathbb{Z}$. Show that $\mathcal{O} = \{x + y\alpha : x, y \in \mathbb{Z}\}$ is a commutative ring with identity.

Presentation Problems

1. (a) Show that $1^2 = 1$ and $(-1)^2 = 1$.
   (b) Show that if R has no zero divisors and if $x \in R$ satisfies $x^2 = 1$ then $x = \pm 1$.
2. Suppose that R is commutative. An element $x \in R$ is called *nilpotent* if $x^m = 0$ for some m.
   (a) Show that if $x, y \in R$ are nilpotent then $x + y$ is nilpotent.
   (b) Show that if $x \in R$ is nilpotent and $y \in R$ is a unit then $x + y$ is a unit.
3. An element x is called *idempotent* if $x^2 = x$. A *Boolean ring* is a ring whose elements are all idempotent.
   (a) Show that every Boolean ring is commutative.
   (b) Classify the Boolean rings that are integral domains.
   (c) Classify the finite Boolean rings.
4. Let R be an integral domain. In this problem, we look at the most efficient way to turn R into a field. Our motivating example will be the construction of $\mathbb{Q}$ from $\mathbb{Z}$ in terms of fractions.

   Consider the set $S = R \times (R \setminus \{0\})$ of pairs of elements of R whose second component is nonzero. We would like to think of a pair $(r, s) \in S$ as a fraction $\frac{r}{s}$, which why we restrict s to be nonzero. There are two steps that we need to take in order to construct our field:

   - Identify fractions that are the same (if $R = \mathbb{Z}$ then $(6, 3)$ and $(4, 2)$ both represent $\frac{2}{1} \in \mathbb{Q}$).
   - Define addition and multiplication on S in a way that respects this identification.

   Recall that when working with rational numbers, $\frac{a}{b} = \frac{c}{d}$ is the same as saying $ad = bc$. This relation, $ad = bc$, is purely a statement about arithmetic in $\mathbb{Z}$.

   In analogy to this, we will define a relation $\sim$ on S by setting $(r_1, s_1) \sim (r_2, s_2)$ whenever $r_1 s_2 = r_2 s_1$.

   (a) Show that $\sim$ is an equivalence relation on S.

   Now let F be the set of equivalence classes of S. We write an equivalence class $[(r, s)]_\sim \in F$ as $\frac{r}{s}$.

   (b) Define a ring structure on F. *Hint*: How do you add and multiply fractions?
   (c) Check carefully that your definitions of addition and multiplication on F preserve $\sim$.
   (d) Show that F is a field.
   (e) Define an injective ring homomorphism $\iota \colon R \to F$.

   Why did we require R to be an integral domain? What do we get if $R = \mathbb{R}[x]$?

   This construction will come up again when we get to Gauss' lemma in section 9.3.

Module Theory Problem

1. Suppose that R is commutative. Read the definition of an R-module and an R-module homomorphism. Convince yourself that R-modules form a category R-Mod. Convince yourself that $\mathbb{Z}$-modules are the same as abelian groups.

   (a) Show that the collection $\mathrm{Hom}_R(M, N)$ of R-module homomorphisms $M \to N$ forms an R-module.

   (b) Show that $\varphi\colon N \to N'$ induces an R-module homomorphism $\varphi_*\colon \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N')$.

   (c) Show that $\varphi\colon M \to M'$ induces an R-module homomorphism $\varphi^*\colon \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N)$.

Tricky Problems

1. Suppose that R is commutative and let $p(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$.

   (a) Show that $p(x)$ is nilpotent if and only if a_j is nilpotent for each $0 \leq j \leq n$.

   (b) Show that $p(x)$ is a unit if and only if a_0 is a unit and a_j is nilpotent for each $1 \leq j \leq n$.

   (c) Show that $p(x)$ is a zero divisor if and only if $bp(x) = 0$ for some nonzero $b \in R$.

   Let $R[[x]]$ denote the ring of formal power series with coefficients in R. Addition is defined by

$$\left(\sum_{n=0}^{\infty} a_nx^n\right) + \left(\sum_{n=0}^{\infty} b_nx^n\right) = \sum_{n=0}^{\infty}(a_n + b_n)x^n$$

   and multiplication is defined by

$$\left(\sum_{n=0}^{\infty} a_nx^n\right)\left(\sum_{n=0}^{\infty} b_nx^n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_kb_{n-k}\right)x^n.$$

   Let $q(x) = a_0 + a_1x + \cdots \in R[[x]]$.

   (d) Show that $q(x)$ is a unit if and only if a_0 is a unit.

   (e) Show that if $q(x)$ is nilpotent then a_j is nilpotent for each $j \geq 0$.

2. Suppose that R is finite and has no zero divisors.

   (a) Show that $R \setminus \{0\}$ forms a group under multiplication.

   (b) Show that there exists a prime number p such that $px = x + x + \cdots + x = 0$ for all $x \in R$.

   (c) Use the classification of finite abelian groups to show that $(R, +) \cong (\mathbb{Z}/p\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p\mathbb{Z})$.

   Now suppose that $|R| = p^2$ and that R is not commutative.

   (d) Show that $Z(R) = \{x \in R\colon xy = yx \text{ for all } y \in R\}$ has order p.

   (e) Let $x \in R \setminus Z(R)$. Show that $C_R(x) = \{y \in R\colon xy = yx\}$ contains both x and $Z(R)$.

   (f) Show that $C_R(x) = R$ and derive a contradiction.