MATH 3032: Abstract Algebra

Assignment 1

due 23 January 2025, end of day

Homework should be submitted as a single PDF attachment to `denisalja@dal.ca`. Please title the file in a useful way, for example `Math3032_HW#_Name.pdf`.

You are encouraged to work with your classmates, but your writing should be your own. If you do work with other people, please acknowledge (by name) whom you worked with. You are expected to attempt every problem on every assignment, but you are not expected to solve every problem on every assignment. The purpose of homework assignments is to learn.

General ring theory

1. Prove that the intersection of any nonempty collection of subrings of a ring is also a subring.
2. Which of the following subsets of $\mathbb{Q}$ are subrings? If the subset is a subring but not a unital subring, then say so. Give *very brief* justifications for your answers.
   (a) The set of all rational numbers with odd denominator when written in lowest terms.
   (b) The set of all rational numbers with even denominator when written in lowest terms.
   (c) The set of all rational numbers with odd numerator when written in lowest terms.
   (d) The set of all rational numbers with even numerator when written in lowest terms.
   (e) The set of all nonnegative rational numbers.
   (f) The set of all squares of rational numbers.
3. Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$, then $x = \pm 1$.
4. Prove that a unital subring of an integral domain is again an integral domain.
5. Let R be a ring. An element $x \in R$ is called *nilpotent* if there is some $n \in \mathbb{N}$ with $x^n = 0$.
   (a) Prove that every nilpotent element is (either zero or) a zero divisor. Conclude that integral domains do not contain nontrivial nilpotent elements.
   (b) Suppose that R is commutative. Prove that if $x, y \in R$ are nilpotent, then so is $x + y$. Prove that if $x \in R$ is nilpotent and $r \in R$ is arbitrary, then rx is nilpotent.
   (c) Prove that if $x \in R$ is nilpotent, then $1 + x$ is invertible (aka a unit).
6. A ring R is *Boolean* if $a^2 = a$ for every $a \in R$.
   (a) Prove every Boolean ring is commutative.
   (b) Prove that if R is Boolean, then $a + a = 0$ for very $a \in R$.
   (c) Show that $\mathbb{Z}/2\mathbb{Z}$ is Boolean.

(d) Let X be any set. Write $\mathcal{P}(X)$ for the *power set* of X: the set of subsets of X. Define the following addition and multiplication laws on $\mathcal{P}(X)$:

$$A + B = (A \cup B) \smallsetminus (A \cap B), \qquad AB = A \cap B.$$

Prove that $\mathcal{P}(X)$ is a Boolean ring.

Geometric algebra

7. Recall that as a set the *complex numbers* $\mathbb{C}$ are $\mathbb{R} \times \mathbb{R}^1$. Let us call a typical complex number "$(a, \vec{v})$" where $a \in \mathbb{R}$ is a scalar, and $\vec{v} = [b] \in \mathbb{R}^1$ is a 1-component vector. This is admittedly a funny notation, but it will make for a good pattern: normally, rather than "$(a, [b])$", we'd write "$a + b\mathbf{i}$." Equip $\mathbb{C}$ with the obvious componentwise additive group law: $(a, \vec{v}) + (a', \vec{v}') = (a + a', \vec{v} + \vec{v}')$. Let $\cdot : \mathbb{R}^1 \times \mathbb{R}^1 \to \mathbb{R}$ denote the usual vector dot product $[b] \cdot [b'] = bb'$. Equip $\mathbb{C}$ with the multiplication law

$$(a, \vec{v})(a', \vec{v}') = (aa' - \vec{v} \cdot \vec{v}', a\vec{v}' + a'\vec{v}).$$

(a) Prove this multiplication law is distributive, unital, and commutative. If these are "obvious," explain why they are obvious. What is the unit element?

(b) Prove that this multiplication law is associative. Conclude that $\mathbb{C}$ is a commutative ring.

(c) Prove that $\mathbb{C}$ is a *division ring*: if $(a, \vec{v}) \neq 0$, then there is an element "$(a, \vec{v})^{-1}$" with $(a, \vec{v})(a, \vec{v})^{-1} = (a, \vec{v})^{-1}(a, \vec{v}) = 1$. Hint: what is the formula for $(a, \vec{v})^{-1}$?

(d) Prove that if we used a "+" sign instead of a "−" sign in the formula for multiplication, then we'd still get a commutative ring, but it would not be a division ring.

(e) Prove that if $n > 1$, then "the same" multiplication law, but now on $\mathbb{R} \times \mathbb{R}^n$, is distributive, commutative, and unital, *but not associative.* Is it a nonassociative division ring?

8. As a set, the *quaternions* $\mathbb{H}$ are $\mathbb{R} \times \mathbb{R}^3$. Let us use the same notation as above, and make $\mathbb{H}$ into an additive group in the obvious componentwise way. (If $\vec{v} = \left[\begin{smallmatrix} b \\ c \\ d \end{smallmatrix}\right]$, then the quaternion $(a, \vec{v})$ is usually written "$a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$".) Recall the *3-dimensional cross product*:

$$\begin{bmatrix} b \\ c \\ d \end{bmatrix} \times \begin{bmatrix} b' \\ c' \\ d' \end{bmatrix} = \begin{bmatrix} cd' - dc' \\ db' - bd' \\ bc' - cb' \end{bmatrix}.$$

Equip $\mathbb{H}$ with the multiplication law

$$(a, \vec{v})(a', \vec{v}') = (aa' - \vec{v} \cdot \vec{v}', a\vec{v}' + a'\vec{v} + \vec{v} \times \vec{v}').$$

(a) Prove that this multiplication law is distributive and unital.

(b) Explain why this multiplication law is not commutative.

(c) Prove that this multiplication law is associative. Conclude that $\mathbb{H}$ is a noncommutative ring.

(d) Prove that $\mathbb{H}$ is a division ring. Hint: what is the formula for $(a, \vec{v})^{-1}$?

9. As a set, the *octonions* $\mathbb{O}$ are $\mathbb{R} \times \mathbb{R}^7$. The *seven-dimensional cross product* is defined by:

$$\begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix} \times \begin{bmatrix} v_1' \\ v_2' \\ v_3' \\ v_4' \\ v_5' \\ v_6' \\ v_7' \end{bmatrix} = \begin{bmatrix} v_2v_3' - v_3v_2' + v_4v_5' - v_5v_4' + v_6v_7' - v_7v_6' \\ v_3v_1' - v_1v_3' + v_5v_7' - v_7v_5' + v_4v_6' - v_6v_4' \\ v_1v_2' - v_2v_1' + v_4v_7' - v_7v_4' + v_6v_5' - v_5v_6' \\ v_5v_1' - v_1v_5' + v_6v_2' - v_2v_6' + v_7v_3' - v_3v_7' \\ v_1v_4' - v_4v_1' + v_7v_2' - v_2v_7' + v_3v_6' - v_6v_3' \\ v_7v_1' - v_1v_7' + v_2v_4' - v_4v_2' + v_5v_3' - v_3v_5' \\ v_1v_6' - v_6v_1' + v_2v_5' - v_5v_2' + v_3v_4' - v_4v_3' \end{bmatrix}$$

(a) Prove that this multiplication law is distributive and unital.

(b) Explain why this multiplication law is not commutative or associative.

(c) Prove that $\mathbb{O}$ is a noncommutative nonassociative division ring.

(d) * Prove the following weaker forms of associativity: for any $x, y \in \mathbb{O}$, we do have

left alternativitity: $x(xy) = (xx)y$

right alternativitity: $x(yy) = (xy)y$

flexibility: $x(yx) = (xy)x$