Math 411: Honors Algebra I
Problem Set 10
due: November 20, 2019

Emily Riehl

Exercise 1. Let R be a ring. Prove that

(i) $u \in R$ is a left unit iff left multiplication by u defines a surjective function $u \cdot - \colon R \to R$.
(ii) If u is a left unit then right multiplication $- \cdot u \colon R \to R$ is also injective (units are not zero divisors).
(iii) The (two-sided) units form a group $R^\times$ under multiplication.

Proof. (i) If $u \cdot -$ is surjective there exists $v \in R$ so that $u \cdot v = 1$. This proves that u is a left unit. Conversely, if u is a left unit, there exists v so that $u \cdot v = 1$. Then $u \cdot (v \cdot a) = (u \cdot v) \cdot a = a$ for any $a \in R$ so $u \cdot -$ is surjective.

(ii) If $a \cdot u = b \cdot u$ and u is a left unit, there exists v so that $u \cdot v = 1$. Now $a = a \cdot u \cdot v = b \cdot u \cdot v = b$ so $- \cdot u$ is injective.

(iii) Suppose u and v are two-sided units (but not necessarily inverses). Then $u \cdot v$ is a two-sided unit with $(uv)^{-1} = v^{-1}u^{-1}$. □

Exercise 2. Prove that if $0 = 1$ in a ring then the ring is the zero ring.

Proof. We saw in class that $0 \cdot r = 0$ for any $r \in R$. So if $0 = 1$ then $0 = 0 \cdot r = 1 \cdot r = r$, which says that the only element is zero. □

Exercise 3. A ring R is **Boolean** if $a^2 = a$ for every $a \in R$.

(i) For any set X prove that the set of subsets of X becomes a Boolean ring with

$$A + B := A \cup B - A \cap B \qquad \text{the symmetric difference}$$
$$A \cdot B := A \cap B \qquad \text{the intersection}$$

by verifying the ring axioms.
(ii) A ring has **characteristic two** if $a + a = 0$ for every $a \in R$. Prove that every Boolean ring has characteristic two.[1]
(iii) Using (ii) prove that every Boolean ring is commutative.[2]

Proof. (i) Clearly $\cap$ is associative with unit X since $X \cap A = A$. This verifies the monoid structure. Note that $A \cap A = A$, which verifies Booleaness.

Note that $+$ is symmetric since $\cup$ and $\cap$ are. The unit for $+$ is $\varnothing$ since $A + \varnothing = A \cup \varnothing - A \cap \varnothing = A$. To see that the addition is associative it's best to draw a venn diagram. The additive inverse for A is A since $A + A = A \cup A - A \cap A = A - A = \varnothing$. This verifies the abelian group structure.

It remains to argue that $\cdot$ distributes over $+$. We compute

$$A \cdot (B + C) = A \cap ((B \cup C) - (B \cap C)) = (A \cap B) \cup (A \cap C) - A \cap B \cap C$$
$$= (A \cap B) \cup (A \cap C) - (A \cap B) \cap (A \cap C) = (A + B) \cdot (A + C).$$

(ii) In a Boolean ring $2a = (a + a) = (a + a)^2 = (2a)^2 = 4a^2 = 4a$. Subtracting we see that $a + a = 2a = 0$.

(iii) In a Boolean ring $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$. Subtracting we see that $ab + ba = 0$, so ba is the additive inverse of ab. But by (ii), ab is the additive inverse of ab so $ab = ba$. □

Exercise 4. Prove or find a counter-example. If R is a ring and $a, b \in R$ are zero divisors then $a + b$ is a zero divisor.

Proof. Note that $[2], [3] \in \mathbb{Z}/6$ are zero divisors but $[2] + [3] = [5]$ is not. □

Exercise 5. Construct a field with 4 elements. The underlying abelian group is $\mathbb{Z}/2 \times \mathbb{Z}/2$ with $(0, 0)$ as the zero element and $(1, 0)$ as the multiplicative identity. The question is to define the multiplication table so that you get a *field* and not just a ring.

[1] Hint: consider $(a + a)^2$.
[2] Hint: consider $(a + b)^2$.

Proof. The underlying abelian group is the Klein four group which has an identity element $e = (0,0)$ and three non-identity elements all of which are interchangeable. So I've renamed the multiplicative identity as $(1,0)$ since it makes no difference. In fact, for ease of type-setting, let's just refer to the four elements as e, i, j, k with e the additive identity and i the multiplicative identity. So far we know part of the multiplication table:

$\cdot$	e	i	j	k
e	e	e	e	e
i	e	i	j	k
j	e	j		
k	e	k		

A ring is a field if and only if its non-zero elements form a group under multiplication. So if we remove the first row and column from the table we should be left with the multiplication table for a group. But we know these are like Sudoku's with each group element appearing exactly once in each row and column. There is only one way to solve this Sudoku, which is

$\cdot$	e	i	j	k
e	e	e	e	e
i	e	i	j	k
j	e	j	k	i
k	e	k	i	j

□

Exercise 6. Let R be a commutative integral domain and consider the polynomial ring $R[x]$. Prove that the only units in $R[x]$ are the constant polynomials $f(x) = a_0$ where a_0 is a unit in R and explain what goes wrong in your proof if R is *not* an integral domain.

Proof. Over an integral domain the product of $f(x) = a_0 + a_1x + \cdots a_nx^n$ with another polynomial will be a polynomial of degree at least n. Since 1 has degree zero, this means that $f(x)$ cannot be a unit unless $n = 0$. Now a constant polynomial $f(x) = a_0$ is a unit iff there exists another constant polynomial $g(x) = b_0$ with $a_0b_0 = 1$, which happens iff $a_0 \in R$ is a unit.

Over a non-integral domain weird things can happen: eg $(1 + 2x)^2 = 1 + 4x + 4x^2 \equiv 1$ in $(\mathbb{Z}/4)[x]$, so $1 + 2x$ is a unit. □

Exercise 7. Let R be a commutative ring and consider the ring of power series $R[\![x]\!]$. Prove that $1 - x$ is a unit in $R[\![x]\!]$ by computing its inverse.[3]

Proof. By direct computation

$$(1 - x) \cdot (\sum_{n\geq 0} a_nx^n) = a_0 + \sum_{n\geq 1}(a_n - a_{n-1})x^n.$$

If we take each $a_n = 1$ then the right hand side is 1, so the inverse to $(1 - x)$ is $\sum_{n\geq 0} x^n$. □

Dept. of Mathematics, Johns Hopkins Univ., 3400 N Charles St, Baltimore, MD 21218
E-mail address: eriehl@math.jhu.edu

[3]More generally, a power series $a_0 + a_1x + a_2x^2 + \cdots$ is a unit in $R[\![x]\!]$ if and only if a_0 is a unit in R.