MA-638 Rings and Fields
Homework for Section 7.1, Jan. 8
Adam Frank

Problem 1. Prove (3) and (4) of Proposition 7.1.

Let R be a ring. Part (3) of Proposition 7.1 is that $(-a)(-b) = ab$ for all $a, b \in R$.

Proof: From part (2) of the same proposition we have that $(-a)(-b) = -(a(-b))$ and then that this equals $a(-(-b))$. If we then show that $b = -(-b)$ the proposition will be proved. This follows by observing that the ring is a group under the additive operation, and we already have that in a group $-(-b) = b$. Hence we have seen that $(-a)(-b) = ab$. $\square$

Part (4) of Proposition 7.1 is that if $\mathbb{1} \in R$ then $-a = (-\mathbb{1})a$.

Proof: For uniqueness, suppose that there are two identities $\mathbb{1}_a$ and $\mathbb{1}_b$. Therefore

$$\mathbb{1}_a \mathbb{1}_b = \mathbb{1}_a = \mathbb{1}_b$$

where the first equality follows from using the identity property of $\mathbb{1}_b$, and the second from using the identity property of $\mathbb{1}_a$.

To show that $-a = (-\mathbb{1})a$, from part (2) again, we have that $(-\mathbb{1})a = -(\mathbb{1}a) = -a$. $\square$

Problem 2. The commutator of an element a in a ring R is defined as $C(a) = \{r \in R | ra = ar\}$ i.e the set of all elements in R that commute with a fixed element a. Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

Proof: That $a \in C(A)$ is immediate from $aa = aa$. Next we show the set is an abelian subgroup under addition. That the addition operation commutes inherits because R is a ring and its addition operation commutes. For closure of addition, if $r, s \in C(a)$ then

$$(r + s)a = ra + sa = ar + as = a(r + s).$$

The first and third equalities are by distributivity, the second by definition of the commutator. To see that the set is closed under additive inverses,

$$(-r)a = -(ra) = -(ar) = a(-r)$$

where the first and last equality are due to Proposition 7.1 part (2). The middle equality is due to the definition of the commutator.

We now have that this set is a group under addition. We complete the proof by showing that the set is closed under multiplication.

$$rsa = ras = ars$$

where each equality is by definition of the commutator. Hence $rs \in C(a)$. Therefore $C(a)$ is a subring of R. □

Let's say that Z is the center of R. We want to show that $Z = \bigcap_{a \in R} C(a)$. We start with showing that $Z \subseteq \bigcap_{a \in R} C(a)$ by showing that any element $x \in Z$ is contained in each $C(a)$ for any $a \in R$. This is immediate since x commutes with every ring element, i.e. for any $a \in R$

$$ax = xa.$$

This satisfies the condition that $x \in C(a)$.

To show that $\bigcap_{a \in R} C(a) \subseteq Z$ we need to show that any two elements of the left-hand set commute with all ring elements. So suppose that $x \in \bigcap_{a \in R} C(a)$

and $r \in R$. Now therefore $x \in C(a)$ for every $a \in R$ and in particular this must hold for r. Hence $x \in C(r)$ and by definition

$$xr = rx.$$

Hence $x \in Z$ and so $\bigcap_{a \in R} C(a) \subseteq Z$. So we have proved $Z = \bigcap_{a \in R} C(a)$. $\square$

Problem 3. Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$, then $x = \pm 1$.

Proof: Immediately we have

$$\begin{aligned} x^2 - 1 &= 0 \\ (x+1)(x-1) &= 0 \end{aligned}$$

where the second equality follows from the first by a routine application of distributivity (twice). Now because R is an integral domain then either $x+1 = 0$ or $x - 1 = 0$. The former implies $x = -1$ and the latter that $x = 1$. $\square$

Problem 4. Suppose that x is a nilpotent element of a commutative ring R.

(a) Prove that x is either zero or a zero divisor.

Proof: By the definition on page 231, we have that there is some smallest $m \in \mathbb{Z}^+$ such that $x^m = 0$. If $x = 0$ there is nothing to prove, so suppose $x \neq 0$ and hence $m > 1$. Then we may write $x^{m-1}x = 0$ with $m - 1 \in \mathbb{Z}^+$. By the minimality of m we must have $x^{m-1} \neq 0$ and so x is a zero divisor. $\square$

(b) Prove that rx is nilpotent for every $r \in R$.

Proof: Again let $m \in \mathbb{Z}$ be such that $x^m = 0$. Since the ring is commutative we have

$$(rx)^m = r^m x^m = r^m \cdot 0 = 0.$$

$\square$

(c) Prove that $\mathbb{1} + x$ is a unit in R.

Proof: Again set $m \in \mathbb{Z}^+$ such that $x^m = 0$. I don't know if there's a more concise proof, but we can observe that

$$x^{m-1}(1 + x) = x^{m-1} + x^m = x^{m-1}.$$

Then

$$\begin{aligned} x^{m-2}(1 + x) = x^{m-2} + x^{m-1} = x^{m-2} + x^{m-1}(1 + x) \quad &\Rightarrow \\ x^{m-2} = (x^{m-2} - x^{m-1})(1 + x) & \end{aligned}$$

and then

$$\begin{aligned} x^{m-3}(1 + x) = x^{m-3} + x^{m-2} = x^{m-3} + (x^{m-2} - x^{m-1})(1 + x) \quad &\Rightarrow \\ x^{m-3} = (x^{m-3} - x^{m-2} + x^{m-1})(1 + x). & \end{aligned}$$

If we continue in this way we eventually find that

$$x^0 = 1 = (1 - x + x^2 - \cdots \pm x^{m-1})(1 + x)$$

which shows that $1 + x$ is a unit.

Problem 5. A ring is called a boolean ring if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

Proof: Since

$$(a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b = a + b$$

then by cancelling and a and b we get

$$\begin{aligned} ab + ba = 0 \quad &\Rightarrow \\ ab = -ba. & \end{aligned}$$

Notice that if $x \in R$ is any ring element then this shows $x^2 = -x^2 = x = -x$ so that every element is its own additive inverse. Hence

$$ab = -(-b)a = ba.$$

□

Problem 6. Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the power set of X). Define addition and multiplication on $\mathcal{P}(X)$ by $A+B=(A\smallsetminus B)\cup(B\smallsetminus A)$ and $A\times B=A\cap B$ i.e., addition is symmetric difference and multiplication is intersection.

(a) Prove that $\mathcal{P}(X)$ is a ring under these operations ($P(X)$ and its subrings are often referred to as rings of sets).

Proof: First we show that it's a commutative group with respect to addition. To show associativity, first simplify

$$\begin{aligned} A+(B+C) &= [A\smallsetminus(B+C)]\cup[(B+C)\smallsetminus A] \\ &= [A\smallsetminus(\{B\smallsetminus C\}\cup\{C\smallsetminus B\})]\cup[(\{B\smallsetminus C\}\cup\{C\smallsetminus B\})\smallsetminus A] \\ &= [(A\smallsetminus\{B\smallsetminus C\})\cap(A\smallsetminus\{C\smallsetminus B\})]\cup \\ &\quad (\{B\smallsetminus C\}\smallsetminus A)\cup(\{C\smallsetminus B\}\smallsetminus A) \end{aligned}$$

Now clearly $\{B\smallsetminus C\}\smallsetminus A=B\cap A^c\cap C^c$ and likewise $\{C\smallsetminus B\}\smallsetminus A=C\cap A^c\cap B^c$. And since

$$\begin{array}{lll} A\smallsetminus(B\smallsetminus C)= & A\cap(B\cap C^c)^c= & A\cap(B^c\cup C) \\ A\smallsetminus(C\smallsetminus B)= & & A\cap(C^c\cup B) \end{array}$$

then

$$\begin{aligned} (A\smallsetminus\{B\smallsetminus C\})\cap(A\smallsetminus\{C\smallsetminus B\}) &= A\cap(B^c\cup C)\cap(C^c\cup B) \\ &= A\cap[(\{B^c\cup C\}\cap C^c)\cup(\{B^c\cup C\}\cap B)] \\ &= A\cap[(B^c\cap C^c)\cup(B\cap C)] \\ &= (A\cap B^c\cap C^c)\cup(A\cap B\cap C) \end{aligned}$$

All of the above then shows

$$\begin{aligned} A+(B+C) = (A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c)\ \cup\ (C\cap A^c\cap B^c)\cup \\ (A\cap B\cap C) \end{aligned}$$

Now to show that this equals $(A + B) + C$ it is enough to show that this is the same thing as $C + (A + B)$, since below I give an independent proof that the operation is commutative. But since what we have above is general, we can apply it to $C + (A + B)$ and see that this equals

$$C + (A + B) = (C \cap A^c \cap B^c) \cup (A \cap C^c \cap B^c) \cup (B \cap A^c \cap B^c) \cup (C \cap A \cap B)$$

Since intersections commute, the two sets are clearly equal.

To show the addition operation is commutative, since

$$A + B = (A \smallsetminus B) \cup (B \smallsetminus A) = (B \smallsetminus A) \cup (A \smallsetminus B) = B + A$$

the addition operation commutes. Of course since $A + B \subseteq X$ then the operation is closed, and all that remains is to show that each element has an inverse. Certainly the zero element of the ring is $\emptyset$ since

$$A + \emptyset = (A \smallsetminus \emptyset) \cup (\emptyset \smallsetminus A) = A \cup \emptyset = A.$$

Therefore we can see that the inverse $-A$ for A is itself. That is to say $A + A = \emptyset$. This follows since

$$A + A = (A \smallsetminus A) \cup (A \smallsetminus A) = \emptyset \cup \emptyset = \emptyset.$$

Now that we have that this is a commutative subgroup for addition, we show that it is closed under multiplication, that multiplication associates, and that multiplication distributes. The first two are trivial since $AB = A \cap B \subseteq X$, and intersections associate. For distributivity,

$$\begin{aligned}
(A \times B) + (A \times C) &= ([A \cap B] \smallsetminus [A \cap C]) \cup ([A \cap C] \smallsetminus [A \cap B]) \\
&= (A \cap B \cap (A \cap C)^c) \cup (A \cap C \cap (A \cap B)^c) \\
&= (A \cap B \cap (A^c \cup C^c)) \cup (A \cap C \cap (A^c \cup B^c)) \\
&= (\emptyset \cup (A \cap B \cap C^c)) \cup (\emptyset \cup (A \cap C \cap B^c)) \\
&= A \cap ([B \smallsetminus C] \cup [C \smallsetminus B]) \\
&= A \times (B + C)
\end{aligned}$$

(b) Prove that this ring is commutative, has identity, and is a Boolean ring.

Proof: That the ring is commutative is trivial since the intersection is a commutative operation on sets: $A \cap B = B \cap A$. The multiplicative identity of any element is the universal set X since

$$AX = A \cap X = A.$$

And the ring is boolean since

$$A^2 = A \cap A = A.$$

□