Homework #11, due 11/18/09 = **7.1.11**, **7.1.15**, **7.1.16**, **7.1.21**, **7.2.12**

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

Assume R is an integral domain and $x^2 = 1$. Then $x^2 - 1 = 0$, so $(x-1)(x+1) = 0$. If both $x - 1$ and $x + 1$ are not zero, then they are both zero divisors. But R has no zero divisors because R is an integral domain. Therefore either $x - 1 = 0$ or $x + 1 = 0$, hence either $x = 1$ or $x = -1$.

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

Assume R is a Boolean ring, so that $a^2 = a$ for every $a \in R$. Let $b, c \in R$. We will show $bc = cb$. First, we note that

$$\begin{aligned} b + c &= (b + c)^2 && R \text{ is Boolean} \\ &= (b + c)(b + c) \\ &= b(b + c) + c(b + c) \\ &= b^2 + bc + cb + c^2 \\ &= b + bc + cb + c && R \text{ is Boolean} \end{aligned}$$

By cancelling b and c from both sides we are left with $0 = bc + cb$, hence $-bc = cb$. However, for every $a \in R$ we have

$$\begin{aligned} -a &= (-a)^2 && R \text{ is Boolean} \\ &= (-a)(-a) \\ &= -a(-a) && \text{Prop. 7.1(2)} \\ &= -(-a^2) && \text{Prop. 7.1(2)} \\ &= a^2 \\ &= a && R \text{ is Boolean} \end{aligned}$$

Therefore, from $-bc = cb$ we get $bc = cb$.

7.1.16 Prove that the only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$.

Assume that R is both an integral domain and a Boolean ring. As a ring, R must contain a multiplicative identity element 1 which is distinct from 0. We will show now that the only two elements of R are 0 and 1. Suppose $a \in R$ and $a \neq 0$. Since R is Boolean, we have $a^2 = a$, hence $0 = a^2 - a = a(a - 1)$. But $a \neq 0$ and R is an integral domain, so there are no zero divisors, hence $a - 1$ must be 0, which implies $a = 1$. Thus 1 is the only nonzero element of R, and we have shown $R = \{0, 1\}$. The additive group of R is therefore the 2-element group $\mathbb{Z}/2\mathbb{Z}$, and the multiplication is completely determined by the properties of 0 and 1: $0 \cdot 0 = 0$, $0 \cdot 1 = 0$, $1 \cdot 0 = 0$, and $1 \cdot 1 =$. Thus R coincides with the 2-element ring $\mathbb{Z}/2\mathbb{Z}$.

7.1.21 Let X be a 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 $A + B = (A - B) \cup (B - A)$ 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 ($\mathcal{P}(X)$ and its subrings are often referred to as *rings of sets*).

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

For every subset $A \subseteq X$, let $\overline{A} = X - A$ be the complement of A. We note some standard set-theoretical laws:

$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
$\overline{\overline{A}} = A$	$A - B = A \cap \overline{B}$
$A \cap \overline{A} = \emptyset$	$\emptyset \cup A = A$
$\cup$ and $\cap$ are associative	$\cup$ and $\cap$ are commutative
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	

Then

$$\begin{aligned} A + B &= (A - B) \cup (B - A) \\ &= (A \cap \overline{B}) \cup (B \cap \overline{A}) \end{aligned}$$

and

$$\begin{aligned} \overline{A + B} &= \overline{(A - B) \cup (B - A)} \\ &= \overline{A - B} \cap \overline{B - A} \\ &= \overline{A \cap \overline{B}} \cap \overline{B \cap \overline{A}} \\ &= (\overline{A} \cup \overline{\overline{B}}) \cap (\overline{B} \cup \overline{\overline{A}}) \\ &= (\overline{A} \cup B) \cap (\overline{B} \cup A) \\ &= (\overline{A} \cap (\overline{B} \cup A)) \cup (B \cap (\overline{B} \cup A)) && \text{dist} \\ &= (\overline{A} \cap \overline{B}) \cup (\overline{A} \cap A) \cup (B \cap \overline{B}) \cup (B \cap A) && \text{dist} \\ &= (\overline{A} \cap \overline{B}) \cup \emptyset \cup \emptyset \cup (B \cap A) \\ &= (\overline{A} \cap \overline{B}) \cup (B \cap A) \end{aligned}$$

Next we use the set-theoretical laws listed above to express both $(A + B) + C$ and $A + (B + C)$ as unions of intersections of sets in $\{A, B, C, \overline{A}, \overline{B}, \overline{C}\}$. The same expression is obtained for both, which proves $(A + B) + C = A + (B + C)$, as follows.

$$\begin{aligned} (A + B) + C &= ((A + B) - C) \cup (C - (A + B)) \\ &= ((A + B) \cap \overline{C}) \cup (C \cap \overline{A + B}) \\ &= (((A \cap \overline{B}) \cup (B \cap \overline{A})) \cap \overline{C}) \cup (C \cap ((\overline{A} \cap \overline{B}) \cup (B \cap A))) \\ &= (((A \cap \overline{B}) \cap \overline{C}) \cup ((B \cap \overline{A}) \cap \overline{C})) \cup ((C \cap (\overline{A} \cap \overline{B}) \cup (C \cap (B \cap A))) \\ &= (A \cap \overline{B} \cap \overline{C}) \cup (B \cap \overline{A} \cap \overline{C}) \cup (C \cap \overline{A} \cap \overline{B}) \cup (C \cap B \cap A) \\ &= (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C) \cup (A \cap B \cap C) \end{aligned}$$

$$\begin{aligned}
A+(B+C) &= (A-(B+C))\cup((B+C)-A)\\
&= (A\cap\overline{B+C})\cup((B+C)\cap\overline{A})\\
&= (A\cap\overline{B+C})\cup(((B\cap\overline{C})\cup(C\cap\overline{B}))\cap\overline{A})\\
&= (A\cap((\overline{B}\cap\overline{C})\cup(C\cap B)))\cup(((B\cap\overline{C})\cup(C\cap\overline{B}))\cap\overline{A})\\
&= (A\cap\overline{B}\cap\overline{C})\cup(A\cap C\cap B)\cup(B\cap\overline{C}\cap\overline{A})\cup(C\cap\overline{B}\cap\overline{A})\\
&= (A\cap\overline{B}\cap\overline{C})\cup(A\cap B\cap C)\cup(\overline{A}\cap B\cap\overline{C})\cup(C\cap\overline{B}\cap\overline{A})\\
&= (A\cap\overline{B}\cap\overline{C})\cup(\overline{A}\cap B\cap\overline{C})\cup(\overline{A}\cap\overline{B}\cap C)\cup(A\cap B\cap C)
\end{aligned}$$

The commutativity of $+$ follows from just the commutativity of $\cup$:

$$A+B=(A-B)\cup(B-A)=(B-A)\cup(A-B)=B+A.$$

The operation $+$ has $\emptyset$ as its identity element, since, for all $A\subseteq X$,

$$A+\emptyset=(A-\emptyset)\cup(\emptyset-A)=A\cup(\emptyset\cap\overline{A})=A\cup\emptyset=A.$$

Every subset $A\subseteq X$ is its own additive inverse, since

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

So far we have shown that $(\mathcal{P}(X),+)$ is an abelian group.

To prove that multiplication (intersection) distributes over $+$ we express both $A(B+C)$ and $AB+BC$ as unions of intersections of sets in $\{A,B,C,\overline{A},\overline{B},\overline{C}\}$. The same expression is obtained for both.

$$\begin{aligned}
A(B+C) &= A\cap((B-C)\cup(C-B))\\
&= A\cap((B\cap\overline{C})\cup(C\cap\overline{B}))\\
&= (A\cap(B\cap\overline{C}))\cup(A\cap(C\cap\overline{B}))\\
&= (A\cap B\cap\overline{C})\cup(A\cap\overline{B}\cap C)
\end{aligned}$$

$$\begin{aligned}
AB+AC &= ((A\cap B)-(A\cap C))\cup((A\cap C)-(A\cap B))\\
&= ((A\cap B)\cap\overline{A\cap C})\cup((A\cap C)\cap\overline{A\cap B})\\
&= ((A\cap B)\cap(\overline{A}\cup\overline{C}))\cup((A\cap C)\cap(\overline{A}\cup\overline{B}))\\
&= ((A\cap B)\cap(\overline{A}\cup\overline{C}))\cup((A\cap C)\cap(\overline{A}\cup\overline{B}))\\
&= ((((A\cap B)\cap\overline{A})\cup((A\cap B)\cap\overline{C})))\cup((((A\cap C)\cap\overline{A})\cup((A\cap C)\cap\overline{B})))\\
&= (\emptyset\cup((A\cap B)\cap\overline{C}))\cup(\emptyset\cup((A\cap C)\cap\overline{B}))\\
&= (A\cap B\cap\overline{C})\cup(A\cap C\cap\overline{B})\\
&= (A\cap B\cap\overline{C})\cup(A\cap\overline{B}\cap C)
\end{aligned}$$

Multiplication is commutative since intersection is commutative, and the set X is also an identity element for multiplication (intersection), since $A\cap X=A$ for every subset $A\subseteq X$. Therefore, $(\mathcal{P}(X),+,\cap)$ is a commutative ring with identity. Finally, $(\mathcal{P}(X),+,\cap)$ is Boolean because, for any subset $A\subseteq X$, $A^2=A\cap A=A$.

7.2.12 Let $G=\{g_1,\ldots,g_n\}$ be a finite group. Prove that the element $N=g_1+g_2+\cdots+g_n$ is in the center of the group ring RG.

The center of a ring R is $\{z\in R|\forall r\in R(zr=rz)\}$, the elements of R that commute with every element of r. In the group ring RG, note that for every $g\in G$ we have $gN=g(g_1+g_2+\cdots+g_n)=gg_1+gg_2+\cdots+gg_n$, but left multiplication by

g is a permutation of the element of G, so $G = \{gg_1, gg_2, \ldots, gg_n\}$, hence $gN = N$. Similarly, $Ng = N$. Consider an arbitrary element $r_1g_1 + \cdots + r_ng_n \in RG$. We have

$$\begin{aligned} N(r_1g_1 + \cdots + r_ng_n) &= r_1Ng_1 + \cdots + r_nNg_n \\ &= r_1N + \cdots + r_nN && Ng = N \\ &= r_1g_1N + \cdots + r_ng_nN && gN = N \\ &= (r_1g_1 + \cdots + r_ng_n)N \end{aligned}$$

which shows N is in the center of RG.