Math 120 Homework 7 Solutions

May 18, 2018

Question 0*

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 operations of addition and multiplication on $\mathcal{P}(X)$ by

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

i.e. addition is the symmetric difference of subsets and multiplication is intersection of subsets. Prove that $\mathcal{P}(X)$ is a commutative ring under these operations.

The additive identity is the empty set $\emptyset$ and the multiplicative identity is the whole set X. The things to check are:

1. $\mathcal{P}(X)$ is closed under addition and multiplication.
2. $(\mathcal{P}(X), +)$ is an abelian group.
3. Multiplication is associative, commutative, and has X as the identity.
4. The distributive property
$$A \times (B + C) = A \times B + A \times C.$$

[TC: One way to understand this in terms of things we discussed in class is to note that $\mathcal{P}(X)$ can be identified with Functions$(X, \mathbb{Z}/2\mathbb{Z})$, where a function $f\colon X \to \mathbb{Z}/2\mathbb{Z}$ corresponds to the set $S_f := \{x \in X \mid f(x) = 1\}$. One should check that the definitions of addition and multiplication above match up (i.e. $S_{f+g} = (S_f \setminus S_g) \cup (S_g \setminus S_f)$ and $S_{f \cdot g} = S_f \cap S_g$), so this is a ring isomorphism.]

Question 1

Let F be a field, and let $R \subset F$ be a subring of F. Prove that R is a domain.

We only need to check that R has no nontrivial zero divisors. Suppose otherwise; then $a \cdot b = 0$ for some $a, b \in R$ both nonzero. Since R is a subring of F, this means that $0 = a \cdot b$ in F as well. But since b is a nonzero element of a field, we know there exists $b^{-1} \in F$ with $b \cdot b^{-1} = 1$. Multiplying the above equation by b^{-1}, we obtain the equality

$$0 = 0 \cdot b^{-1} = a \cdot b \cdot b^{-1} = a \cdot 1 = a$$

in F. This contradicts our assumption that a is nonzero.

Question 2

Suppose that R is a domain, and $x \in R$ satisfies $x^2 = 1$. Prove that $x = 1$ or $x = -1$.

Let $x \in R$ be any element satisfying $x^2 = 1$. Consider the element $y = (x-1)(x+1)$. Using distributivity, we can write

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

by applying the distributive property twice. Thus, $y = (x-1)(x+1) = 0$. Since R is a domain, it has no nontrivial zero divisors, so either $x - 1 = 0$ or $x + 1 = 0$. Therefore $x = 1$ or $x = -1$ respectively.

Question 3

Construct a ring K with the property that for every ring R, the number of ring homomorphisms $\varphi : K \to R$ is equal to the cardinality $|R|$.

Let $K = \mathbb{Z}[x]$, the ring of polynomials with integer coefficients, multiplied in the usual way. Then, it suffices to show that the homomorphisms $\varphi : K \to R$ are in one-to-one correspondence with the elements of R. The key is that a homomorphism $\varphi\colon \mathbb{Z}[x] \to R$ is uniquely determined by the image $\varphi(x)$, and conversely, for any element $r \in R$ there exists a homomorphism with $\varphi_r(x) = r$. We handle the latter claim first.

Given an element $r \in R$, define the map $\varphi_r : K \to R$ by

$$\varphi_r(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i r^i$$

for any integers $a_i \in \mathbb{Z}$, $0 \leq i \leq n$. It is easy to check that this map is a ring homomorphism. The claim is that (a) these φ_r are all distinct and (b) every $\varphi : K \to R$ is one of them.

To prove (a), note that $\varphi_r(x) = r$, so if $r \neq r'$ then $\varphi_r(x) \neq \varphi_{r'}(x)$.

To prove (b), let $\varphi : K \to R$ be a ring homomorphism, and take $r = \varphi(x)$. We claim that $\varphi = \varphi_r$. In fact, since φ is a ring homomorphism,

$$\begin{aligned} \varphi(\sum_{i=0}^{n} a_i x^i) &= \sum_{i=0}^{n} \varphi(a_i)\varphi(x)^i \\ &= \sum_{i=0}^{n} a_i r^i, \end{aligned}$$

since ring homomorphisms respect addition and multiplication and always fix the integers. Thus, $\varphi(\sum a_i x^i) = \varphi_r(\sum a_i x^i)$ for every element $\sum a_i x^i \in \mathbb{Z}[x]$, and we are done.

Question 4

An element $r \in R$ is called *idempotent* if $r^2 = r$.

(a*) Let A and B be commutative rings. Check that in the product ring $A \times B$, the element $(1, 0) \in A \times B$ is idempotent.

Multiplication in the product ring is coordinatewise, so $(1, 0)^2 = (1^2, 0^2) = (1, 0)$.

(b) (Hard) Prove that if R is commutative and $x \in R$ is an idempotent with $x \neq 0$ and $x \neq 1$, then there exist commutative rings A and B such that $R \simeq A \times B$.

Define $y = 1 - x$. Then, because x is idempotent,

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

so y is also idempotent. Define Rx to be the set $\{rx : r \in R\}$ (this is called the *ideal* generated by x), and Ry similarly. We claim that Rx and Ry are commutative rings for which $R \simeq Rx \times Ry$.

First, we check that Rx is a commutative ring if x is an idempotent. One important point is that the multiplicative identity will *now be* x. (In particular, Rx is *not* a subring; but it is a ring under multiplication.) Note that it is closed under addition, since $ax+bx=(a+b)x$, and multiplication, since $ax\cdot bx=abx^2=abx$. The element x is indeed the multiplicative identity, since $ax\cdot x=ax^2=ax$. Because R is commutative Rx is automatically commutative.

Thus, Rx and Ry are both commutative rings. Define $\phi: R\to Rx\times Ry$ by sending $\phi(a)=(ax,ay)$. We claim that ϕ is a ring isomorphism, with inverse given by $\psi: Rx\times Ry\to R$ sending $\psi((u,v))=u+v$.

It is easy to check that ϕ and ψ are homomorphisms; the only interesting bit is what happens to identities. We have $\phi(1)=(x,y)$ which is indeed the identity in the product, since x is the identity in Rx and y is the identity in Ry. For ψ, we have $\psi(x,y)=x+y=1$ since $y=1-x$.

Also,

$$\psi\circ\phi(a)=\psi((ax,ay))=ax+ay=a(x+y)=a,$$

and

$$\phi\circ\psi((u,v))=\phi(u+v)=((u+v)x,(u+v)y)=(ux+vx,uy+vy)$$

Note that since $u\in Rx$ and $v\in Ry$, $ux=u$ and $vy=v$. Meanwhile,

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

so $uy=0$ and $vx=0$. Thus,

$$\phi\circ\psi((u,v))=(u,v).$$

We have shown that ψ and ϕ are mutually inverse ring homomorphisms, so $R\simeq Rx\times Ry$, as desired.

(c) Prove that if A and B are domains, the ring $R=A\times B$ contains exactly 4 idempotents.

The four are $(0,0),(0,1),(1,0),(1,1)$. Let $(a,b)\in R$ be any idempotent of R. Then,

$$(a^2,b^2)=(a,b)^2=(a,b).$$

Then, $a^2=a$ and $b^2=b$, so a is an idempotent in A and b is an idempotent in B. But in a domain, the only idempotents are 0 and 1. If any other element x was an idempotent, $x(1-x)=x-x^2=0$, so there would be nontrivial zero divisors $x,1-x$. Thus, a,b are both either 0 or 1, and $(a,b)\in\{(0,0),(0,1),(1,0),(1,1)\}$, as desired. This is an exhaustive list of idempotents in $A\times B$.

(d) (Hard, Optional) If R is the ring of infinite-integers from HW6, find domains A and B such that $R\simeq A\times B$. Can you describe A and B explicitly? How much can you say about them? In what ways are they like R, or different from R?

The idempotents $x,y\in R$ that you found have the property that, in a suitable sense, x is not divisible by 5 but is divisible by every power of 2 and y is not divisible by 2 but is divisible by every power of 5. It follows by part (b) that $R\simeq(a)\times(b)$. It turns out that just as R is the ring of "infinite integers in base 10," (a) is isomorphic to the ring of "infinite integers in base 5" and (b) is isomorphic to ring of the "infinite integers in base 2."

Question 5

For any $X\subseteq\mathbb{R}$, we can define the ring $C(X)$ of continuous real-valued functions on X:

$$C(X)=\{f: X\to\mathbb{R} | f \textbf{ is continuous}\}.$$

The ring structure comes from pointwise addition and multiplication: the functions $g=f_1+f_2$ and $h=f_1\cdot f_2$ are defined by

$$\begin{aligned} g(x) &= f_1(x)+f_2(x)\\ h(x) &= f_1(x)\cdot f_2(x) \end{aligned}$$

(You may assume without proof that $C(X)$ is a ring.)

Recall from elementary school that if $f : \mathbb{R} \to \mathbb{R}$ is a function on the whole real line, we can *restrict* f to a smaller set such as $[0, 1]$ to obtain $f|_{[0,1]} : [0, 1] \to \mathbb{R}$.

In fact, for any $X \subsetneq Y$, we can restrict functions $f : Y \to \mathbb{R}$ to obtain a function $f|_X : X \to \mathbb{R}$. If we write $r(f) = f|_X$, this defines a restriction map $r : C(Y) \to C(X)$. (You may assume without proof that $r : C(Y) \to C(X)$ is a ring homomorphism.)

(a) Give an example of two sets $X \subsetneq Y \subseteq \mathbb{R}$ such that $r : C(Y) \to C(X)$ is surjective.

Take $Y = \mathbb{R}$ and $X = \{0\}$ the single point. Then the restriction map $r : C(\mathbb{R}) \to C(\{0\})$ is just evaluation of functions. This is surjective because for every value $r \in \mathbb{R}$ there is a continuous function on $\mathbb{R}$ with $f(0) = r$, e.g. the constant function $f(x) = r$.

(b) Give an example of two sets $X \subsetneq Y \subseteq \mathbb{R}$ such that $r : C(Y) \to C(X)$ is not surjective.

Take $Y = [0, 1]$ and $X = [0, 1)$. The function $f = 1/(1 - x)$ lies in $C(X)$ but cannot be extended to a continuous function on $[0, 1]$, since $f(x) \to \infty$ as $x \to 1^-$. Thus f is not in the image of r.

(c) Give an example of two sets $X \subsetneq Y \subseteq \mathbb{R}$ such that $r : C(Y) \to C(X)$ is injective.

Take $Y = [0, 1]$ and $X = [0, 1)$ again. To show that r is injective, it suffices to show that $r(f) = 0$ implies $f = 0$. This is true because $f(1) = \lim_{x\to 1^-} f(x)$, so if $f(x) = 0$ on all of X then $f(1) = 0$ as well, so $f = 0$ in Y.

(d) Give an example of two sets $X \subsetneq Y \subseteq \mathbb{R}$ such that $r : C(Y) \to C(X)$ is not injective.

Take $Y = \mathbb{R}$ and $X = \{0\}$ the single point again. The nonzero function $f(x) = x$ in $C(Y)$ is mapped to 0 in $C(X)$.

(e) (Optional) Is it possible to find two sets$X \subsetneq Y \subseteq \mathbb{R}$ such that $r : C(Y) \to C(X)$ is an isomorphism? Either give an example or sketch a proof that it is impossible.

No, this is impossible. If r is an isomorphism, then it is both surjective and injective. We will first show that if r is injective, then Y is a subset of the closure of X, in other words every point of Y is the limit of a sequence of points in X.

If not, then there exists a point $y \in Y$ and a small open interval $(y - \epsilon, y + \epsilon)$ around it which doesn't intersect X. But then we can define a continuous bump function $f_y : \mathbb{R} \to \mathbb{R}$ which is nonzero at y and zero outside the interval $(y-\epsilon, y+\epsilon)$. This function's restriction to Y is nonzero, but $r(f_y|_Y) = 0$ since $f_y(x) = 0$ on all of $x \in X$. Thus r would not be injective if Y were not a subset of the closure of X.

Now, pick any $y \in Y \backslash X$, and consider the continuous function $g_y(x) = 1/(x - y)$ which is defined on X because $y \notin X$. We claim that g_y is not in the image of $r : C(Y) \to C(X)$, so r is not surjective.

Since Y is in the closure of X, y is the limit of some sequence $(x_n)_{n\geq 1}$ of points in X. If a function $g \in C(Y)$ restricted to $g_y(x)$, then $g(y) = \lim_{n\to\infty} g_y(x_n) = \infty$ by continuity. Thus, no real-valued function in $C(Y)$ restricts to g_y, as desired.