MATH 3032: Abstract Algebra

Assignment 1

Solutions

1. **Let R be a ring, and $n \in \mathbb{Z}$ an integer. Recall that, for every $x \in R$, there is a well-defined element "$n \cdot x$," defined in terms of the additive group structure on R.**

   For a positive integer n, we say that R has *characteristic* n if $n \cdot x = 0$ for all $x \in R$ and n is the smallest positive integer with this property. If there does not exist a positive integer n such that $n \cdot x = 0$ for all $x \in R$, then we say that R has *characteristic* 0.

   (a) **Show that $\mathbb{Z}_n$ has characteristic n.**

   Indeed, pick $m \in \mathbb{Z}_n$, and let $\tilde{m} \in \mathbb{Z}$ be a representative. The product $n \cdot m \in \mathbb{Z}_n$ is the residue mod n of the integer $n\tilde{m}$, which is obviously divisible by n. This shows that the "for all" part of the definition is satisfied. To show that n is the minimal positive number with the stated property, note that if $n' < n$ is also positive, then n does not divide n', and so $n' \cdot 1 \neq 0$ in $\mathbb{Z}_n$.

   (b) **Show that the zero ring is the unique unital ring of characteristic 1.**

   We need to confirm that the zero ring does have charateristic 1. But if $x \in \{0\}$, then $x = 0$, so $1 \cdot x = 1 \cdot 0 = 0$. So $n = 1$ satisfies the conditions of the definition, and there are no smaller positive integers than 1 full stop (satisfing the condition of not).

   (c) **Give an example of a nonunital ring of characteristic 1 other than the zero ring.**

   The statement is obviously wrong. Indeed, $1 \cdot x = x$. So if $x = 0$ for all $x \in R$, then R contains only one element, and is the zero ring.

   (d) **Suppose that R is unital, with unit 1_R. Show that R has characteristic n if and only $n \cdot 1_R = 0$.**

   If R is unital of characteristic n, then certainly $n \cdot 1_R = 0$, since $1_R \in R$ is an example of an element. It suffices to show the converse. But the distributive law shows that for any elements $x, y \in R$ in any ring, $n \cdot (xy) = (n \cdot x)y$. Specializing x to 1_R, we see that, for every $y \in R$, $n \cdot y = n \cdot (1_R y) = (n \cdot 1_R)y = 0y = 0$.

   The exercise has a missing statement: the conditions in the exercise are not enough to guarantee that n is minimal. The exercise should add that n is the minimal value for which $n \cdot 1_R = 0$. Then certainly there cannot be a smaller n' for which $n' \cdot x = 0 \, \forall x$.

2. **Recall that a ring R is called *Boolean* if for every $x \in R$, $x^2 = x$.**

   (a) **Show that every Boolean ring is commutative.**

Let R be Boolean and $x, y \in R$. We want to show that $xy = yx$. Consider the element $x + y$. By using the Boolean axioms three times, together with distributivity, we find:

$$x + y = (x + y)^2 = (x + y)(x + y) = x^2 + yx + xy + y^2 = x + yx + xy + y.$$

We can now subtract to conclude

$$xy = -yx.$$

On the other hand, by the next question, for any $z \in R$, $z = -z$, and so in particular $-yx = yx$.

(b) **Show that every Boolean ring has characteristic (1 or) 2.**

Let R be a Boolean ring. We want to show that $2x = 0$ for all x. But, since R is Boolean, $(2x)^2 = 2x$, whereas whether R was Boolean or not we would have $(2x)^2 = 4x$. Using $x^2 = x$, we then find $2x = 4x$. Subtracting $2x$ from both sides gives the final answer.

3. **The following notion is not normally covered in undergraduate textbooks, but is quite important to some research applications. (For example, it came up in my current research.)**

Let R be a ring. Then R is called *von Neumann regular* (vN regular) if for every $x \in R$, there exists a $y \in R$ such that $xyx = x$.

(a) **Show that every division ring is vN regular.**

Suppose R is a division ring and $x \in R$. If $x = 0$, then taking $y = 0$ obviously fulfills the condition. If $x \neq 0$, then taking $y = x^{-1}$ obviously fulfills the condition.

(b) **Show that every Boolean ring is vN regular.**

If R is Boolean and $x \in R$, then taking $y = x$ obviously works.

(c) **Is the zero ring vN regular?**

Yes. $0^3 = 0$.

(d) **Is $\mathbb{Z}$ vN regular?**

No. Take, for example, $x = 2$. Then for any $y \in \mathbb{Z}$, $xyx = 4y$ is divisible by 4. Since 2 is not divisible by 4, this will never equal 2.

(e) **Is $\mathbb{Z}_{10}$ vN regular?**

Yes, somewhat remarkably. One way to demonstrate this is simply to go through all classes mod 10 and check. Here is a more general approach.

Let $n = pq$ with $p \neq q$ both prime. (In the case at hand, $n = 10$, $p = 2$, and $q = 5$.) Let $x \in \mathbb{Z}_n$. By the Chinese Remainder Theorem, we can find a, b such that $x = aq + bp$, and the classes of $a \mod p$ and of $b \mod q$ are uniquely determined by x. Since p is prime, if $a \neq 0 \mod p$, then we can find a' such that $aa' = 1 \mod p$; similarly, if $b \neq 0 \mod q$, then we can find b' such that $bb' = 1 \mod q$. If $a = 0 \mod p$, then set $a' = 0$, and if $b = 0 \mod q$, then set $b' = 0$. Finally, set $y = a'q + b'p$. Then

$$xy = (aq + bp)(a'q + b'p) = aa'q + bb'p + (ab' + a'b)qp = aa'q + bb'p \mod n.$$

Similarly,

$$xyx = a^2a'q + b^2b'p \mod n.$$

Now, if $a = 0 \mod p$, then $a^2a'q = 0 \mod pq$, whereas if $a \neq 0 \mod p$, then $a^2a' = a \mod p$, so $a^2a'q = a \mod pq$. Ditto for the bs, and so $xyx = x$.

(f) **Is $\mathbb{Z}_8$ vN regular?**

No. An element of $\mathbb{Z}_8$ has a well-defined modulus mod 4, and 2 is not divisible by 4 in $\mathbb{Z}_8$. So we can repeat the answer from item (c).

(g) [Bonus problem — hard!] **Is the ring $C(\mathbb{R})$ of continuous functions $\mathbb{R} \to \mathbb{R}$ vN regular?**

No, suppose that $f \in C(\mathbb{R})$ is sometimes 0 and sometimes not 0. Suppose further that there was some g for which $fgf = f$. Then, at any $x \in \mathbb{R}$ for which $f(x) \neq 0$, we'd have to have $f(x)g(x)f(x) = f(x)$, and dividing by $f(x)$ gives $g(x) = f(x)^{-1}$ for those values. Now, because f is sometimes zero and sometimes non-zero, we can find a convergent sequence $x_1, x_2, \dots$ in $\mathbb{R}$ such that $f(x_n) \neq 0$ for all x_n, whereas $f(\lim_{n\to\infty} x_n) = 0$. But then the sequence $g(x_n)$ cannot have a limit, so the putative g would not be continuous.

4. **Recall that an *idempotent* in a ring R is an element $p \in R$ such that $p^2 = p$. For example, 0 is an idempotent, and if R is unital, then 1 is also an idempotent. An idempotent other than 0 or 1 is called a *nontrivial idempotent*.**

(a) **Show that, if R is a division ring, then all idempotents are trivial.**

Suppose that R is a division ring and that $p \in R$ is idempotent. If $p = 0$ then p is trivial. Otherwise p is invertible, and so dividing both sides of the equation $p^2 = p$ by p gives $p = 1$, so p is trivial.

(b) **Show that, in $\mathbb{Z}$, all idempotents are trivial.**

The argument in part (a) only required that multiplication be cancelative.

(c) **Find a nontrivial idempotent in $\mathbb{Z}_{15}$. (There are two of them.)**

We can try all cases, or use the Chinese Remainder Theorem. The latter says that p is idempotent mod 15 if and only if it is idempotent mod 3 and mod 5. Modulo a prime, part (a) shows that all idempotents are trivial. If p is going to be nontrivial overall, then we want a number which is $1 \mod 3$ but $0 \mod 5$, or a number which is $0 \mod 3$ but $1 \mod 5$. In other words: $p = 10$ and $p = 6$ work. Let's check this: $10^2 = 100 = 90 + 10 = 6 \times 15 + 10 = 10 \mod 15$; $6^2 = 36 = 30 + 6 = 2 \times 15 + 6 = 6 \mod 15$.

(d) **Suppose that R is commutative and that $p \in R$ is an idempotent. Define subsets $\ker(p) \subset R$ and $\operatorname{im}(p) \subset R$ as follows:**

$$\ker(p) := \{x \in R \textbf{ s.t. } xp = 0\}, \qquad \operatorname{im}(p) := \{x \in R \textbf{ s.t. } xp = x\}.$$

Show that every element $z \in R$ is uniquely expressible as $z = x + y$ with $x \in \ker(p)$ and $y \in \operatorname{im}(p)$.

Suppose we can find $z = x + y$ with $x \in \ker(p)$ and $y \in \operatorname{im}(p)$, i.e. with $xp = 0$ and $yp = y$. Then multiplying by p gives

$$zp = xp + yp = 0 + y$$

and so

$$y = zp, \qquad x = z - zp.$$

This shows uniqueness of x, y. It also shows existence, because for these choices of x, y,

$$yp = (zp)p = zp^2 = zp = y, \qquad xp = (z-zp)p = zp-zp^2 = zp-zp = 0, \qquad z = (z-zp)+zp.$$

(e) **Show that** $\ker(p)$ **and** $\operatorname{im}(p)$ **are subrings of** R**.**

We consider obvious the fact that these are abelian subgroups, as this just follows from the fact that, for fixed p, the equations $xp = 0$ and $xp = x$ are linear in x. The interesting part is that $\ker(p)$ and $\operatorname{im}(p)$ are closed under multiplication in R. But they are in fact ideals: if $y \in R$ is arbitrary and x solves $xp = 0$, then $(yx)p = y(xp) = y0 = 0$; if $y \in R$ is arbitrary and x solves $xp = x$, then $(yx)p = y(xp) = yx$.

(f) **Show that** $\operatorname{im}(p)$ **is unital as a ring. Show that, if** R **is unital, then** $\ker(p)$ **is unital as a ring. But show that if** p **is nontrivial, then neither** $\operatorname{im}(p)$ **nor** $\ker(p)$ **is a unital subring of** R**.**

The unit in $\operatorname{im}(p)$ is p itself. Indeed, $p \in \operatorname{im}(p)$, from the defining equation $p^2 = p$, and if $x \in \operatorname{im}(p)$, then certainly $xp = x$.

If R is moreover unital, then $1 - p \in \ker(p)$ because $(1 - p)p = p - p^2 = 0$, and $1 - p$ is the unit in $\ker(p)$ because $x(1 - p) = x - xp = 0$ if $x \in \ker(p)$.

If $p \neq 0, 1$, then neither p nor $1 - p$ is equal to 1. So these are not unital subrings.

(g) **Show that the function** $R \to \operatorname{im}(p)$ **sending** $x \mapsto xp$ **is a ring homomorphism, and that it is a unital ring homomorphism if** R **is unital.**

We first show that $x \mapsto xp$ does define a function $R \to \operatorname{im}(p)$: $(xp)p = xp^2 = xp$, so the image is in $\operatorname{im}(p)$. If R is unital, then this function manifestly sends $1 \mapsto p$, so it is a unital function. We must check that it is a multiplicative map. But, using commutativity,

$$(xp)(yp) = xyp^2 = (xy)p$$

for all $x, y \in R$.