Math 566 - Homework 1
SOLUTIONS
Prof Arturo Magidin

1. Let $(R,+,\cdot)$ be a ring, and define the *opposite ring* $(R^{\mathrm{op}},+,\circ)$ as follows: the underlying set of R^{op} is R, and addition in R^{op} is the same as addition on R. Multiplication on R^{op}, which we will denote by $\circ$, is defined by $a\circ b = b\cdot a$, where $\cdot$ is the multiplication in R.

   (i) Show that $(R^{\mathrm{op}},+,\circ)$ is a ring.
   Proof. That R^{op} is an abelian group follows because we did not change the addition operation.
   So we just need to verify the properties of multiplication. We have:
   - $a\circ(b\circ c) = (b\circ c)a = (cb)a = c(ba) = (ba)\circ c = (a\circ b)\circ c$, so $\circ$ is associative.
   - $a\circ(b+c) = (b+c)a = ba+ca = a\circ b + a\circ c$; so $\circ$ distributes on the left.
   - $(b+c)\circ a = a(b+c) = ab+ac = b\circ a + c\circ a$, so $\circ$ distributes on the right.

   Thus, R^{op} is a ring. $\Box$

   (ii) Show that R has an identity if and only if R^{op} has an identity.
   Proof. If 1_R is an identity for R, then $a\circ 1_R = 1_R a = a$ and $1_R\circ a = a1_R = a$, so 1_R is an identity for R^{op}. Since $(R^{\mathrm{op}})^{\mathrm{op}} = R$, the converse now follows as well. $\Box$

   (iii) Show that R is a division ring if and only if R^{op} is a division ring.
   Proof. Let $a\in R^{\mathrm{op}}$ be nonzero. If a^{-1} is the multiplicative inverse of a in R, then $a^{-1}\circ a = aa^{-1} = 1_R$ and $a\circ a^{-1} = a^{-1}a = 1_R$, so a^{-1} is also a $\circ$-inverse for a in R^{op}. Thus, every nonzero element of R^{op} has an inverse, so R^{op} is a division ring. The converse again follows because $(R^{\mathrm{op}})^{\mathrm{op}} = R$. $\Box$

2. Let $(R,+,\cdot)$ be a set, together with two binary operations, and assume that the set and operations satisfy all the axioms of a ring, *except perhaps* for commutativity of addition. That is, $(R,+)$ is a (not necessarily commutative) group, $\cdot$ is associative, and $\cdot$ distributes on both sides over $+$.

   (i) Prove that if R has a multiplicative identity, i.e., an element $1_R\in R$ such that $a\cdot 1_R = 1_R\cdot a = a$ for all $a\in R$, then $x+y=y+x$ for all $x,y\in R$; that is, commutativity of $+$ is a consequence of the other axioms of a ring, together with the existence of a unity.
   Proof. Let $x,y\in R$. Consider $(x+y)(1_R+1_R)$ distributed both ways:
   $$\begin{aligned}(x+y)(1_R+1_R) &= (x+y)1_R + (x+y)1_R = x+y+x+y\\ (x+y)(1_R+1_R) &= x(1_R+1_R) + y(1_R+1_R) = x+x+y+y.\end{aligned}$$
   Since these two are equal, we have $x+y+x+y = x+x+y+y$. Adding $-x$ on the left and $-y$ on the right, we obtain $y+x = x+y$. Thus, addition is necessarily commutative in this situation. $\Box$

   (ii) Give an example to show that commutativity of $+$ does not follow from the other axioms if R does not have a multiplicative identity, by exhibiting an example of a set R, and binary operations $+$ and $\cdot$ such that $(R,+)$ is a *nonabelian* group, and $\cdot$ is an associative operation that distributes over $+$ on both sides.
   Answer. Let G be a nonabelian group (written multiplicatively). Define $(R,+,\cdot)$ by letting R be the same set as G, and defining $a+b=ab$ and $a\cdot b = e_G$. This satisfies all conditions of a ring except for commutativity of $+$; indeed, we have a group under $+$, and
   $$\begin{aligned}(a\cdot b)\cdot c &= e_G = a\cdot(b\cdot c),\\ a\cdot(b+c) &= e_G = e_Ge_G = (a\cdot b)+(a\cdot c),\\ (a+b)\cdot c &= e_G = e_Ge_G = (a\cdot c)+(b\cdot c). \quad \Box\end{aligned}$$

3. **Cayley's Theorem for Rings.** Let $(R, +, \cdot)$ be a ring; for each $r \in R$, let $\lambda_r \colon R \to R$ be the function given by

$$\lambda_r(a) = ra$$

   (i) Show that for each $r \in R$, λ_r is an element of $\mathrm{End}(R, +)$, the endomorphism group of the abelian group $(R, +)$.

   Proof. We just need to show that $\lambda_r(a + b) = \lambda_r(a) + \lambda_r(b)$; but this is just the left distributivity of multiplication: $r(a + b) = ra + rb$. $\square$

   (ii) Define $\psi \colon R \to \mathrm{End}(R, +)$ by $\psi(r) = \lambda_r$. Prove that this map is a ring homomorphism (where $\mathrm{End}(R, +)$ is a ring with pointwise addition and composition of functions). Prove that if R has a unity, then ψ is one-to-one.

   Proof. We have that for all $r, s \in R$, and each $a \in R$,

$$\begin{aligned}
\psi(r+s)(a) &= \lambda_{r+s}(a) = (r+s)a = ra + sa = \lambda_r(a) + \lambda_s(a)\\
&= (\lambda_r + \lambda_s)(a) = (\psi(r) + \psi(s))(a).\\
\psi(rs)(a) &= \lambda_{rs}(a) = (rs)a = r(sa) = r(\lambda_s(a))\\
&= \lambda_r(\lambda_s(a)) = (\lambda_r \circ \lambda_s)(a) = (\psi(r) \circ \psi(s))(a).
\end{aligned}$$

   Thus, $\psi(r + s) = \psi(r) + \psi(s)$ and $\psi(rs) = \psi(r) \circ \psi(s)$. Thus, ψ is a ring homomorphism.

   If R has a unity and $r \in \ker(\psi)$, then $\psi(r)$ is the zero map, so $r = r1_R = \psi(r)(1_R) = 0$. Thus, $\ker(\psi) = \{0\}$, proving that ψ is one-to-one.

   Alternatively: if R has a unity, and $\psi(r) = \psi(s)$, then

$$r = r1_R = \lambda_r(1_R) = \psi(r)(1_R) = \psi(s)(1_R) = \lambda_s(1_R) = s1_R = s,$$

   hence $\psi(r) = \psi(s)$ implies $r = s$, so ψ is one-to-one, as claimed. $\square$

   (iii) Use the Dorroh embedding to show that if R is a ring, with or without unity, then there exists an abelian group A an a one-to-one ring homomorphism $\varphi \colon R \to \mathrm{End}(A, +)$. That is: every ring is [isomorphic to] a subring of the endomorphism ring of an abelian group.

   Proof. Let R be a ring. If R has a unity, then part (ii) already yields that R embeds into the endomorphism ring of the abelian group $(R, +)$.

   If R does not have a unity, then we know that R embeds into the ring with unity S constructed using the Dorroh embedding. Now, the map $\psi \colon S \to \mathrm{End}(S)$ from part (ii) is a ring embedding. Thus, the composition $\psi \circ h \colon R \to \mathrm{End}(S)$ gives the desired embedding. $\square$

   Note: In fact, the latter construction can be done to *any* ring, whether or not it has a unity. If R already has a unity, then this embeds it as a subring into a new ring with a new unity.

4. A *Boolean ring* is a ring $(R, +, \cdot)$ such that $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative and $a = -a$ for all $a \in R$. *Hint:* Square $(a + a)$ and $(a - b)$. (An element a of a ring such that $a^2 = a$ is called an *idempotent*.)

   Proof. We have

$$\begin{aligned}
(a + a) &= (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a\\
(a - b) &= (a - b)^2 = a^2 - ab - ba + b^2 = a - ab - ba + b.
\end{aligned}$$

   From the first equality, cancelling we get $a + a = 0$, so $a = -a$. This holds for all $a \in R$, and so in particular we also have $ab = -ab$ for any $a, b \in R$. Thus, in the second equation we have

$$a + b = a - b = a - ab - ba + b = a + ab + ba + b.$$

   Cancelling again, we get $ab + ba = 0$, so $ab = -ba = ba$. Thus, $ab = ba$ and so the ring is commutative. $\square$

5. Let X be a set, and let $\mathcal{P}(X)$ be the power set of X (the set of all subsets of X). Define operations $\oplus$ and $\odot$ on $\mathcal{P}(X)$ by:

$$\begin{aligned} A \oplus B &= (A - B) \cup (B - A) && \text{(symmetric difference)} \\ A \odot B &= A \cap B && \text{(intersection)} \end{aligned}$$

Show that $(\mathcal{P}(X), \oplus, \odot)$ is a Boolean ring with unity.

Proof. The symmetric difference is commutative and associative: $(A \oplus B) \oplus C$ consists exactly of the elements that are in exactly one of A, B, and C, or in all three; the same holds for $A \oplus (B \oplus C)$.

The empty set is the additive identity: $A \oplus \varnothing = (A - \varnothing) \cup (\varnothing - A) = A$. Finally, A is the additive inverse of A, since $A \oplus A = (A - A) \cup (A - A) = \varnothing$.

The intersection is associative; the set X is a multiplicative identity. Since intersection distributes over union, we have that

$$A \odot (B \oplus C) = A \cap ((B - C) \cup (C - B)) = (A \cap (B - C)) \cup (A \cap (C - B)).$$

On the other hand,

$$(A \odot B) \oplus (A \odot C) = \Big((A \cap B) - (A \cap C)\Big) \cup \Big((A \cap C) - (A \cap B)\Big).$$

Now we simply note that $R \cap (S - T) = (R \cap S) - (R \cap T)$. Indeed, if $a \in R \cap (S - T)$ then $a \in R$, $a \in S$, and $a \notin T$; therefore, $a \in R \cap S$ and $a \notin R \cap T$, so $a \in (R \cap S) - (R \cap T)$. Conversely, if $x \in (R \cap S) - (R \cap T)$, then $x \in R \cap S$ and $x \notin R \cap T$; thus, $x \in R$, $x \in S$, and either $x \notin R$ or $x \notin T$. Since $x \notin R$ is impossible, we get $x \in R$, $x \in S$, and $x \notin T$; that is, $x \in R \cap (S - T)$.

Thus, we get the equality we seek and we have a ring with unity. Finally, $A \odot A = A \cap A = A$, so we have a boolean ring. $\square$

6. Give an example of a ring R and a subring S such that R has a unity, S has a unity, but $1_S \neq 1_R$.

Answer. Let $R = \mathbb{Z} \times \mathbb{Z}$; the unity of R is $(1, 1)$. Let $S = \mathbb{Z} \times \{0\}$. This is a subring; and $(1, 0) \in S$ is a unity for S. So R is a ring, S is a subring of R, R has a unity, S has a unity, but $1_S = (1, 0) \neq (1, 1) = 1_R$. $\square$