THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Tutorial 8 Solutions
18th March 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

1. We will verify that $(R^\times, \times)$ is a group.

   (1) Closedness (well-definedness) of binary operation: Let $r, s \in R^\times$, then r^{-1}, s^{-1} exists, note that $(rs)(s^{-1}r^{-1}) = (s^{-1}r^{-1})(rs) = 1_R$, so that $rs \in R^\times$.

   (2) Associativity: It follows from the definition of ring that $\times$ is associative on R, so it is also associative when restricted to $R^\times$.

   (3) Existence of identity and inverse: The identity element is given by the multiplicative identity 1_R of R, indeed $r \times 1_R = 1_R \times r = r$. The inverse of an element $r \in R^\times$ is given by r^{-1} as guaranteed by the definition of $R^\times$. Note that r^{-1} is only assumed to be in R, it is in fact in $R^\times$ because $rr^{-1} = r^{-1}r = 1_R$ implies that $(r^{-1})^{-1} = r$ exists.

   (a) $\mathbb{Z}_{20}^\times = \{k \in \mathbb{Z}_{20} : \gcd(k, 20) = 1\} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. Indeed, we can prove that in general, $\mathbb{Z}_n^\times = \{k \in \mathbb{Z}_n : \gcd(k, n) = 1\}$. For the $\subseteq$ inclusion, note that if k has a multiplicative inverse in $\mathbb{Z}_n$, then there exists l such that $kl \equiv 1$ modulo n, in other words $kl + nm = 1$ for some $m, l \in \mathbb{Z}$. Since $\gcd(k, n)$ divides $kl + nm$, this implies that $\gcd(k, n)$ divides 1, so it must be equal to 1.

   For the $\supseteq$ inclusion, if $\gcd(k, n) = 1$, then we can find $m, l \in \mathbb{Z}$ so that $kl + nm = \gcd(k, n) = 1$. This fact actually follows from Euclidean algorithm in $\mathbb{Z}$, which you may take for granted. In particular, the equation implies that $kl \equiv 1$ modulo n. Therefore k has a multiplicative inverse in the ring $\mathbb{Z}_n$.

   (b) By definition $M_{n\times n}(\mathbb{C}) = \{A \in M_{n\times n}(\mathbb{C}) : \exists B, AB = BA = I_n\} = GL_n(\mathbb{C})$ is the group of invertible matrices with coefficients in $\mathbb{C}$.

   (c) Let R be an integral domain, consider the degree function $\deg : R[x] \setminus \{0\} \to \mathbb{N}$ where $\deg(f(x))$ is defined as the largest n such that the coefficient of x^n is nonzero. Note that $\deg(fg) = \deg(f) + \deg(g)$, since if $a_n x^n$ and $b_m x^m$ are the leading terms of f and g respectively, then $a_n b_m x^{n+m}$ is the leading term of fg, as $a_n b_m$ is nonzero since R is an integral domain. Let $f(x) \in R[x]^\times$, there exists $g(x)$ so that $f(x)g(x) = 1_R$ (the multiplicative identity of 1_R, when regarded as an element of $R[x]$ is the multiplicative identity). So $\deg(f) + \deg(g) = \deg(1_R) = 0$, which implies that $\deg(f) = \deg(g) = 0$, so $f, g \in R$. Therefore

   $$R[x]^\times = \{f(x) \in R[x] : \exists g, f(x)g(x) = 1_R\} = \{r \in R : \exists s, rs = sr = 1_R\} = R^\times.$$

   Remark: The set of units in $R[x]$ in general for R not an integral domain is more complicated. An element $r \in R$ is called nilpotent if $r^n = 0$ for some $n > 0$. Then $R[x]^\times$ in general is given by $f(x) = a_0 + a_1 x + ... + a_n x^n$ such that $a_0 \in R^\times$ and $a_1, ..., a_n \in R$ are nilpotent.

2. To verify that $(\mathrm{End}(G), +, \circ)$ is a ring, we have to verify the following properties:

   (1) $(\mathrm{End}(G), +)$ is an abelian group: $+$ indeed defines a binary operation on R, since $\varphi+\psi$ is still an endomorphism, by courtesy of the fact that G is abelian. The associativity of $+$ follows from associativity of product of G. And the operation is abelian since G is abelian. The identity (i.e. additive identity) is given by $0(g) := e$ for all $g \in G$. This endormophism satisfies $(\varphi + 0)(g) = (0 + \varphi)(g) = \varphi(g)$. Therefore the additive inverse of a $\varphi \in R$ is given by $-\varphi(g) := \varphi(g)^{-1}$, again this is a well-defined homomorphism since G is abelian.

   (2) $\circ$ defines an associative binary operation on $\mathrm{End}(G)$ with multiplicative identity: The associativity follows from that of composition. And the multiplicative identity 1 is just given by $1 = \mathrm{id}$ the identity homomorphism.

   (3) Finally, we have to verify the distributive law. If φ, ψ, σ are in R, then $(\varphi+\psi)\circ\sigma(g) = (\varphi + \psi)(\sigma(g)) = \varphi(\sigma(g))\psi(\sigma(g)) = (\varphi \circ \sigma + \psi \circ \sigma)(g)$. The other distributive law is similar.

   We claim that $(\mathrm{End}(\mathbb{Z}_p), +, \circ) \cong (\mathbb{Z}_p, +, \times)$. Note that this is an isomorphism of rings (you will learn about this soon, and you may come back to reread this part later), on the RHS, we have the ring of integers modulo p, while the LHS involves the ring structure coming from composition of group homomorphisms. The map is explicitly given by $F : \mathrm{End}(\mathbb{Z}_p) \to (\mathbb{Z}_p, +, \times)$ defined by $F(\varphi) = \varphi(1)$. This is a ring homomorphism since $F(\varphi + \psi) = (\varphi + \psi)(1) = \varphi(1) + \psi(1)$, and $F(1_{\mathrm{End}(G)}) = \mathrm{id}(1) = 1$ which is the multiplicative identity in $\mathbb{Z}_p$. We also have $F(\varphi \circ \sigma) = (\varphi \circ \sigma)(1) = \varphi(\sigma(1))$. We may write $k = \sigma(1)$ for some $0 \leq k \leq p - 1$, then $\varphi(\sigma(1)) = \varphi(k) = \varphi(\underbrace{1 + ... + 1}_{k \text{ times}}) = \varphi(1) \cdot k = \varphi(1)\sigma(1)$. It remains to check that F is bijective. In fact, one can construct an inverse homomorphism $G : (\mathbb{Z}_p, +, \times) \to (\mathrm{End}(G), +, \circ)$ by $G(k) = \varphi_k : 1 \mapsto k$, where $k \in \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a cyclic group, so it is determined by the image of 1. It is a simple exercise to verify that $F(G(k)) = k$ and $G(F(\varphi)) = \varphi$.

   Some comments: $\mathrm{End}(G)$ is an important example of a ring. The endomorphism ring of an abelian group is the ring-theoretic analogue of symmetric group of a set. Remember when we learnt about groups, a lot of emphasis was put into explaining how one may understand certain groups as symmetries of some sets (for example, a group may act on set of left cosets of a subgroup). The idea is that groups are understood by its action on sets, whereas rings are understood by its action on abelian groups. A ring acting on an abelian group is known as a module, it is a generalization of a vector space, where the ring is replaced by a field. The theory of modules is a rich and deep subject that is both related to representation theory and algebraic geometry.

   Proposition. Let $(R, +, \times)$ be a ring, then R is isomorphic to a subring of an endormorphism ring.

   Proof. Let $r \in R$, then r defines a group homomorphism $L_r : (R, +) \to (R, +)$ by $L_r(x) = rx$ for any $x \in R$. Distributive law says that this is a homomorphism. Therefore we can try to define $\varphi : R \to \mathrm{End}(R, +)$ by $\varphi(r) = L_r$. One can easily check that it is a ring homomorphism by verifying $L_{r+s} = L_r + L_s$ and $L_{rs} = L_r \circ L_s$. This ring homomorphism is injective because $L_r = \mathrm{id}$ in particular implies that $r1 = r = \mathrm{id}(1) = 1$.

3. Let R be a finite commutative ring, if u is not a zero divisor, then consider the set $\{u, u^2, u^3, ...\}$. This is a subset of R, hence it is finite. So by the pigeonhole principle there are $i < i + k$ so that $u^i = u^{i+k}$. Therefore $u^i(u^k - 1) = 0$. We will show that since u is not zero divisor, u^i is also not a zero divisor. If u^i was a zero divisor, then $u^i b = 0$ for some $b \neq 0$, then $u(u^{i-1}b) = 0$. Now u is not a zero divisor, this forces $u^{i-1}b = 0$. Inductively, this reduces to $ub = 0$ for some $b \neq 0$, this contradicts with u being not a zero divisor. So $u^i(u^k - 1) = 0$ is possible only if $u^k = 1$. In particular u^{k-1} is the inverse to u, so it is invertible.

4. A lot of the ring axioms for $R \times S$ boil down to direct checking. For example $R \times S$ is an abelian group because it coincides with how we defined the product group back then. The multiplicative identity of $R \times S$ is given by $(1_R, 1_S)$. And the distributive law follows from that of R and S. For example, $((r, s) + (u, v)) * (x, y) = (r + u, s + v) * (x, y) = ((r + u) * x, (s + v) * y) = (r * x + u * x, s * y + v * y) = (r * x, s * y) + (u * x, v * y) = (r, s) * (x, y) + (u, v) * (x, y)$.

   We can explicitly find zero divisors in $R \times S$, for example $(1_R, 0_S) * (0_R, 1_S) = (0_R, 0_S)$ shows that $(1_R, 0_S)$ is a zero divisor. So product rings are never integral domains.

5. (a) We verify the various axioms:

   (1) $(P(S), +)$ is an abelian group: The addition as defined is abelian since $\cup$ and $\cap$ are abelian. The additive identity is given by $0 = \emptyset$, since $0 + A = A + 0 = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A$. The additive inverse of $A \in P(S)$ is A itself since $A + A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset$. The most tricky part is the associativity. First note that $A + B$ is the symmetric difference of A and B, i.e. $A + B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \sqcup (B \setminus A) = (A \cap B^c) \sqcup (B \cap A^c)$, where $A^c = S \setminus A$ denotes the complement of C. Note that

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

   Here in the last equality, we have used that $(A \cup B)^c = A^c \cap B^c$ and that intersection distributes over union of sets. Note that the expression we have obtained is symmetric with respect to A, B, C. In particular, it is equal to $(B + C) + A$, this in turns is equal to $A + (B + C)$ by commutativity, so we are done.

   (2) The multiplicative identity is given by $1 = S$, since $1 * A = A * 1 = A \cap S = A$ for any $A \in P(S)$. The multiplication is clearly associative.

   (3) Distributive laws: This follows from that fact that $(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C)$

$$\begin{aligned}
A * C + B * C &= (A \cap C) + (B \cap C) \\
&= [(A \cap C) \setminus (B \cap C)] \sqcup [(B \cap C) \setminus (A \cap C)] \\
&= [(A \setminus B) \cap C] \sqcup [(B \setminus A) \cap C] \\
&= [(A \setminus B) \sqcup (B \setminus A)] \cap C \\
&= (A + B) * C.
\end{aligned}$$

   The other distributive law follows from the one above since both $+, *$ are commutative.

(b) We have already shown above that $A + A = 0$. And clearly $A * A = A \cap A = A$.

(c) Any element in $(\mathbb{Z}/2\mathbb{Z})^n$ is of the form $(a_1, ..., a_n)$ where $a_i \in \mathbb{Z}/2\mathbb{Z}$. Note that $a_i = 0$ or 1 and both of them satisfy $x * x = x$. Therefore in the product ring, $(a_1, ..., a_n)^2 = (a_1^2, ..., a_n^2) = (a_1, ..., a_n)$ still holds true.

(d) Let R be a Boolean ring, then $x * x = x$ for any $x \in R$. Let $x, y \in R$, consider $(x + y)^2 = x + y$. Expanding the LHS gives $x^2 + xy + yx + y^2 = x + xy + yx + y$. This implies that $xy + yx = 0$. Now we will show that $a + a = 0$ for any $a \in R$, then $a = -a$ and therefore we obtain $xy = -yx = yx$.

Simply consider $a + a = (a + a)^2 = (a^2 + a^2 + a^2 + a^2) = a + a + a + a$. Moving $a + a$ to the RHS, gives $a + a = 0$, as desired.

If R is an integral domain, since every element satisfies $x^2 = x$. We may write $x(x - 1) = 0$. By property of integral domain, we must have $x = 0$ or $x = 1$. Therefore, every element is either 1 or 0, so $R \cong \mathbb{Z}/2\mathbb{Z}$.