THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 6 Solutions
21st March 2024

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

Compulsory Part

1. (a) Let $n \in \mathbb{Z}$, then $n \in \mathbb{Z}^\times$ iff there exists m such that $nm = 1$, this holds precisely when $n = \pm 1$. So $\mathbb{Z}^\times = \{1, -1\}$.

   (b) Note that the multiplicative identity function is $\mathbb{1} : \mathbb{R} \to \mathbb{R}$ where $\mathbb{1}(x) = 1$ for any $x \in \mathbb{R}$. A real-valued function f on $\mathbb{R}$ is invertible if there exists g such that $f(x)g(x) = \mathbb{1}(x) = 1$ for any $x \in \mathbb{R}$. In particular, for any $x \in \mathbb{R}$, $f(x) \in \mathbb{R}$ is invertible in the field $\mathbb{R}$, so $f(x) \neq 0$. Conversely, if $f(x) \neq 0$ for any x, then by taking $g(x) = 1/f(x)$, we see that g is a multiplicative inverse to $f(x)$. Thus $R^\times = \{f : \mathbb{R} \to \mathbb{R} |\, f(x) \neq 0, \, \forall x \in \mathbb{R}\}$.

   (c) Let D be an integral domain, we will show that $D[x]^\times = D^\times$. Let $f(x) \in D[x]^\times$, let $g(x) \in D[x]$ such that $f(x)g(x) = 1$. Then $\deg(f) + \deg(g) = \deg(1) = 0$, so that $\deg(f) = \deg(g) = 0$, i.e. $f(x)$ and $g(x)$ are constant polynomial, and we may regard $f(x) = a, g(x) = b \in D$. Then $f(x)g(x) = ab = 1$ may be regarded as an equation in D. In particular, a, b are invertible. So $f(x) = a \in D^\times$.

2. $R^\times$ is a group under multiplication since multiplication is a well-defined associative binary operation by definition of ring, and any element $r \in R^\times$ by definition has an inverse under this operation. The multiplicative identity 1 of R, satisfies $1 \cdot 1 = 1$, and so $1 \in R^\times$. It is by definition the identity under product, therefore it forms a group.

3. We will prove the statement by induction on n, the case for $n = 1$ is clear as both sides are exactly the same. Suppose that the equality has been shown for some $n \in \mathbb{Z}_{>0}$, consider

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{l=0}^{n} \binom{n}{l} a^{n-l} b^{l+1} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k \\
&= \binom{n}{0} a^{n+1} + \binom{n}{n} b^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n+1-k} b^k \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.
\end{aligned}$$

In the last equality, we have used the equality $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$, which can be shown directly from

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{(n-k+1)\cdot n!}{k!(n-k+1)!} + \frac{k\cdot n!}{k!(n-k+1)!} \\ &= \frac{(n-k+1+k)\cdot n!}{k!(n-k+1)!} \\ &= \frac{(n+1)!}{k!(n-k+1)!} \\ &= \binom{n+1}{k}.\end{aligned}$$

Therefore, the equality holds true for arbitrary n.

4. If a, b are nilpotent, suppose $a^n = 0$ and $b^m = 0$ for some $n, m \in \mathbb{Z}_{>0}$, note that in the solution of Q3, we only used the fact that a commutes with b. Therefore, by the same argument, we have
$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k.$$
Note that for $k = 0, 1, ..., m$, we have $a^{n+m-k}b^k = a^n \cdot (a^{m-k}b^k) = 0 \cdot (a^{m-k}b^k) = 0$ and for $k = m+1, m+2, ..., m+n$, we have $a^{n+m-k}b^k = b^m(a^{n+m-k}b^{k-m}) = 0 \cdot (a^{n+m-k}b^{m-k}) = 0$. Therefore, each term in the above sum is zero, this implies that $(a+b)^{n+m} = 0$ and thus $a+b$ is nilpotent.

5. (a) Note that it suffices to show that $na = 0$ for all $a \in D$ if and only if $n1 = 0$. Then in particular, there is no n such that $na = 0$ for all $a \in D$ if and only if there is no n so that $n1 = 0$. And the minimums of n satisfying both conditions are the same.

   If $na = 0$ for all $a \in D$, then in particular taking $a = 1$, we get $n1 = 0$.

   Conversely, if $n1 = 0$, then $na = a + a + ... + a = 1 \cdot a + 1 \cdot a + ... + 1 \cdot a = (1 + 1 + ... + 1) \cdot a = n1 \cdot a = 0 \cdot a = 0$. This completes the proof.

   (b) If D has nonzero characteristic, suppose that it has characteristic n, if n was not prime, then $n = kl$ for some $k, l > 1$. Then $0 = n1 = k1 \cdot l1$. Since $k, l \neq n$, $k1$ and $l1$ are nonzero element whose product is zero, which contradicts to the fact that D is an integral domain.

Optional Part

1. Note that $(a+b)(a-b) = a(a-b) + b(a-b) = a^2 - b^2 + ba - ab = a^2 - b^2$ holds true if and only if $ba = ab$. Therefore $(a+b)(a-b) = a^2 - b^2$ for all $a, b \in R$ if and only if $ab = ba$ for all $a, b \in R$, i.e. R is commutative.

2. No, both $2, 3$ are zero divisors in $\mathbb{Z}_6$ since $2 \cdot 3 = 0$ but $2 + 3 = 5$ is a unit in $\mathbb{Z}_6$.

For another example, consider the ring $M_2(\mathbb{R})$ the ring of 2-by-2 matrices with real coefficients, then the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are zero divisors since their product is the zero matrix, but they sum to give the identity matrix, which is not a zero divisor.

3. See Q5d of tutorial 8.

4. (a) Let f, g be real valued function so that $f(0) = g(0) = 0$, then clearly $f + g$ is also a real valued function, and $(f + g)(0) = f(0) + g(0) = 0$, so $f + g \in R$.

   (b) Similarly $(fg)(0) = f(0)g(0) = 0$, so $fg \in R$.

   (c) The additive identity is given by the zero function $\mathbb{0}(x) := 0$ for all $x \in \mathbb{R}$ then by definition $\mathbb{0} \in R$. Clearly $(\mathbb{0} + f)(x) = 0 + f(x) = f(x) = (f + \mathbb{0})(x)$, so that $\mathbb{0} + f = f + \mathbb{0} = f$ so it is the additive identity.

   (d) The multiplicative identity is given by the function $\mathbb{1}(x) := 1$ for all $x \neq 0$ and $\mathbb{1}(0) = 0$. By definition $\mathbb{1} \in R$, and $(\mathbb{1} \cdot f)(x) = f(x)$ for all $x \neq 0$, and for $x = 0$, $\mathbb{1}(0)f(0) = 0 = f(0)$. So we have verified that $\mathbb{1} \cdot f = f \cdot \mathbb{1} = f$ for all f, so it is the multiplicatively identity.

5. (a) Yes, let $a, b \in R$ be units, then there exists a^{-1}, b^{-1} so that $aa^{-1} = a^{-1}a = 1 = bb^{-1} = b^{-1}b$. Then $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1$, so ab is also a unit.

   (b) No, 1 is unit in $\mathbb{Z}_2$ but $1 + 1 = 0$ is not a unit.

6. ($\Rightarrow$) If $R[x]$ is an integral domain, note that $\varphi : R \to R[x]$ by sending any $r \in R$ to r regarded as a constant polynomial is a well-defined injective ring homomorphism, i.e. we may regard $R \subset R[x]$ as a subring. Now a subring of an integral domain must be an integral domain, otherwise zero divisors in R will give zero divisors in $R[x]$.

   ($\Leftarrow$) If R is an integral domain, we will show that $R[x]$ does not contain zero divisors as well. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$ be general elements in $R[x]$, expressed in the form such that a_n, b_m are nonzero, assume that $f(x)g(x) = 0 \in R[x]$, then $f(x)g(x) = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j x^k = 0$. Here $\sum_{i+j=k} a_i b_j$ is the coefficient of x^k in $f(x)g(x)$. In particular the coefficient of x^{n+m} is $a_n b_m = 0$, which implies that a_n or b_m is zero, as R does not contain zero divisor. This contradicts with our assumption on a_n and b_m.

7. (a) If f or g is 0, then $\deg(fg) = \deg 0 = -\infty$ and $\deg f + \deg g = -\infty$ since $\deg f$ or $\deg g$ is $-\infty$. (Let's say we are doing arithmetic over $[-\infty, \infty)$ where $-\infty + k = -\infty$ for any finite k.)

   Now if f, g are nonzero, then the degree is defined as the the maximum power appearing in the finite sum $f(x) = \sum_{i=0}^{\infty} a_i x^i$, i.e. the index n such that $a_n \neq 0$ but $a_i = 0$ for all $i > n$. Suppose that $\deg(f) = n$ and $\deg(g) = m$, then we may write $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$. where a_n and b_m are nonzero. Then $f(x)g(x) = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j x^k$. Clearly there are no terms with higher degree than $m + n$, and the coefficient for x^{m+n} is given by $a_n b_m$, which is nonzero since R is an integral domain. Therefore $\deg(fg) = m + n = \deg f + \deg g$.

   (b) If f or g is zero, say $f = 0$ wlog, then $f + g = g$ and $\deg(f + g) = \deg g$ so the inequality holds true.

Now suppose f, g are nonzero, we may write $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty}$, and suppose f, g have degrees n, m respectively, i.e. $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. Then $f \pm g = \sum_{i=0}^{\infty} (a_i \pm b_i) x^i$. For $i > \max\{n, m\}$, clearly $a_i \pm b_i = 0$ since $a_i = b_i = 0$. thus $\deg(f \pm g) \leq \max\{m, n\}$.