THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Tutorial 9 Solutions
25th March 2024

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

1. Let I, J be ideals, in particular they are additive subgroups of $(R, +)$. Then $I \cap J$ is again an additive subgroup, since the intersection of subgroups is again one. Let $r \in R$ and $x \in I \cap J$, then $x \in I$ and $x \in J$, so that $rx, xr \in I$ and also in J, so they are in $I \cap J$.

   Similarly, $I + J$ is an additive subgroup since if $x = a + b, y = c + d \in I + J$, then $x - y = (a + b) - (c + d) = (a - c) + (b - d) \in I + J$. Now let $x = a + b \in I + J$ and $r \in R$, then $r \cdot x = ra + rb$ and $x \cdot r = ar + br$. Since I, J are ideals, $ra, ar \in I$ and $rb, br \in J$, so that $r \cdot x$ and $x \cdot r$ are in $I + J$.

2. Let I_i be an ascending chain of ideals in R, if $a, b \in I := \bigcup_{i=1}^{\infty} I_i$, then there exists a large enough n so that $a, b \in I_n$, so $a - b \in I_n \subset I$. So I is an additive subgroup. Now if $r \in R$, $x \in I$, then $x \in I_n$ for some n, then rx and xr are in $I_n \subset I$.

3. Let $r \in R$ and $\sum_{i=1}^{n} a_i s_i, \sum_{j=1}^{m} b_j s'_j \in \langle S \rangle$, then WLOG we may assume that $s_i = s'_j$ for $i = j$, otherwise we may simply relabel the s'_j. Then $\sum_{i=1}^{n} a_i s_i - \sum_{j=1}^{m} b_j s_j = \sum_{i=1}^{\max m,n} (a_i - b_i) s_i \in \langle S \rangle$, where we define s_i and s'_j to be zero if $i > n$ and $j > m$. This shows that $\langle S \rangle$ is an additive subgroup. Also, $(\sum_{i=1}^{n} a_i s_i) \cdot r = r \cdot \sum_{i=1}^{n} a_i s_i = \sum_{i=1}^{n} (r a_i) s_i \in \langle S \rangle$, since R is assumed to be commutative. Therefore $\langle S \rangle$ is an ideal. Note that $\langle S \rangle$ as defined may not be an ideal if R was not assumed to be commutative.

   If I is any ideal so that $S \subset I$, then by property of ideal, $\sum_{i=1} a_i s_i \in I$. In particular, this implies that $\langle S \rangle \subset \bigcap_{S \subset I} I$. Conversely, $\langle S \rangle$ is an ideal so that $S \subset \langle S \rangle$, therefore $\bigcap_{S \subset I} I \subset \langle S \rangle$ since it is one of the ideals that we are taking intersection of.

   If J is some ideal so that $S \subset J$, then $\langle S \rangle = \bigcap_{S \subset I} I \subset J$.

4. Let $I \subset \mathbb{Z}$ be a nontrivial ideal, let $n > 0$ be the smallest positive number in I. Since $n \in I$, we have $a \cdot n \in I$ for any $a \in \mathbb{Z}$, so that $n\mathbb{Z} \subset I$.

   On the other hand, if $x \in I$ is a nonzero integer, since $x \in I$ if and only if $-x \in I$, we may assume that $x > 0$, by Euclidean algorithm, we have $x = kn + r$ where $k \geq 0$ and $n > r \geq 0$. Now $x, n \in I$, so that $r = x - kn \in I$, this forces $r = 0$ since we assumed that n is the smallest positive integer in I. So we obtain $x = kn$, i.e. $x \in n\mathbb{Z}$.

5. (a) Suppose that R has characteristic $n > 0$, then $n \cdot r = n \cdot (1_R \times_R r) = (n \cdot 1_R) \times_R r = 0_R \times_R r = 0_R$.

   (b) Suppose R does not contain a zero divisor, if R has characteristic $n > 0$, then $\varphi(n) = n \cdot 1_R = 0_R$ by assumption. If $n = ab$ for some positive integers a, b, then $0_R = \varphi(n) = \varphi(ab) = \varphi(a)\varphi(b)$. This forces $\varphi(a) = 0_R$ or $\varphi(b) = 0_R$ since R does not contain zero divisor. Then $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$, i.e. a or b is a multiple of n. This implies that n is a prime number, since a, b are arbitrary integer factors of n.

(c) To show that f is a ring homomorphism, note that $f(x+y) = (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$, note that the coefficients $\binom{p}{i}$ are divisible by p for $i = 1, 2, ..., p-1$. By (a), this implies that $\binom{p}{i} x^i y^{p-i} = 0_R$ for $i = 1, 2, ..., p-1$. So that $f(x+y) = x^p + y^p = f(x) + f(y)$. We also have $f(xy) = (xy)^p = x^p y^p = f(x)f(y)$ since R is commutative. And $f(1_R) = 1_R^p = 1_R$.

If R is an integral domain, then $f(x) = x^p = 0_R$ only if $x = 0_R$, otherwise R has a zero divisor. Therefore $\ker(f) = \{0_R\}$ so f is injective.

6. Define $\varphi : \mathbb{Z}[x] \to R$ by $\varphi(x) = a$ and $\varphi(1) = 1_R$, this determines $\varphi(p(x))$ for any $p(x) \in \mathbb{Z}[x]$ since we may write $p(x) = \sum_{i=0}^{n} c_i x^i$, then $\varphi(p(x)) = \varphi(\sum_{i=0}^{n} c_i x^i) = \sum_{i=0}^{n} \varphi(c_i)\varphi(x)^i = \sum_{i=0}^{n} c_i a^i = p(a)$. Here, c_i refers to the element $c_i 1_R \in R$. It is clear that when defined this way, φ is indeed a ring homomorphism from the formula $\varphi(p(x)) = p(a)$.

   Now if R' is a subring of R so that $a \in R'$, then by property of subring, $1_R \in R'$ and any products of $a \in R$. Therefore if $p(x) \in \mathbb{Z}[x]$ is a polynomial, then $p(a) = \sum_{i=0}^{n} c_i a \in R'$. This shows that $\mathrm{im}(\varphi) \subset R'$.

7. Let $r, s \in \mathrm{Nil}(R)$, then $r^n = 0_R = s^m$ for some $m, n > 0$. Then $(-r)^n = (-1)^n r^n = 0_R$ so $-r \in \mathrm{Nil}(R)$. And $(r+s)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} r^i s^{m+n-i}$. Note that each term of the sum contains r^i for $i \geq n$ or s^j for $j \geq m$. Therefore each term is 0_R, and $(r+s)^{m+n} = 0_R$, this shows that $r + s \in \mathrm{Nil}(R)$. Now if $a \in R$ is any element, $(ra)^n = (ar)^n = a^n r^n = 0_R$ as well, so $\mathrm{Nil}(R)$ forms an ideal.