**THE CHINESE UNIVERSITY OF HONG KONG**
**Department of Mathematics**
**MATH 3030 Abstract Algebra 2023-24**
**Homework 8**
**Due Date: 23th November 2023**

## Compulsory Part

1. Prove that if $D$ is an integral domain, then $D[x]$ is an integral domain.

   *Proof.* Let $D$ be an integral domain. Then $D$ is a commutative ring with unity $1 = 1_D$, and $D$ has no zero divisors. Then $D[x]$ is also a commutative ring with unity $1_{D[x]} = 1_D$. Let $f, g \in D[x]$. Suppose $f \neq 0, g \neq 0$. Then $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, $g = b_m x^m + b_{m-1}x^{m-1} + ... + b_0$ for some $a_i, b_j \in D$ with $a_n, b_m \neq 0$. Then $a_n b_m \neq 0$ since $D$ is an integral domain. Then the leading term of $fg$ is $a_n b_m x^{m+n}$, which is nonzero. Then $fg \neq 0$. It follows that $D[x]$ is an integral domain. □

2. Let $D$ be an integral domain and $x$ an indeterminate.

   (a) Describe the units in $D[x]$.

   (b) Find the units in $\mathbb{Z}[x]$.

   (c) Find the units in $\mathbb{Z}_7[x]$.

   *Proof.* (a) The units in $D[x]$ are exactly the units in $D$: $D[x]^\times = D^\times$. We give a proof here:

   For $a \in D^\times$, $ab = 1$ for some $b \in D$. Since $a, b \in D[x]$, this implies that $a \in D[x]^\times$. Conversely, let $f \in D[x]^\times$, then $fg = 1$ for some $g \in D[x]$. Then $\deg(f) + \deg(g) = \deg(1) = 0$. Then $\deg(f) = \deg(g) = 0$, and so $f, g \in D$. Therefore, $f \in D^\times$.

   (b) By (a), $\mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{\pm 1\}$

   (c) By (a), $\mathbb{Z}_7[x]^\times = \mathbb{Z}_7^\times = \mathbb{Z}_7 - \{0\}$.

   □

3. Let $R$ be a commutative ring with unity of prime characteristic $p$. Show that the map $\phi_p : R \to R$ given by $\phi_p(a) = a^p$ is a ring homomorphism (called the **Frobenius homomorphism**).

   *Proof.* Let $R$ be a commutative ring with unity of prime characteristic $p$. Let $\phi_p : R \to R$ be given by $\phi_p(a) = a^p$. Then $\phi_p(1) = 1^p = 1$. For any $a, b \in R$, $\phi_p(ab) = (ab)^p = a^p b^p = \phi_p(a)\phi_p(b)$ because $R$ is commutative.

   On the other hand, $\phi_p(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$. Note that for $1 \leq i \leq p-1$, $p | \binom{p}{i}$, and so $\binom{p}{i} = 1$ in $R$ because char$(R) = p$. Then $\phi_p(a+b) = (a+b)^p = a^p + b^p = \phi_p(a) + \phi_p(b)$.

   It follows that $\phi_p$ is a ring homomorphism. □

4. Show that for $p$ a prime, the polynomial $x^p + a$ in $\mathbb{Z}_p[x]$ is reducible for any $a \in \mathbb{Z}_p$.

   *Proof.* Let $p$ be a prime, and let $a \in \mathbb{Z}_p$. Let $\phi_p : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$ be the map as in Q3. Then $\phi$ is a ring homomorphism because $\text{char}(\mathbb{Z}_p[x]) = p$. By Fermat's little theorem, $\phi(a) = a^p = a$ in $\mathbb{Z}_p$. Then $x^p + a = \phi_p(x) + \phi_p(a) = \phi_p(x + a) = (x + a)^p$. Therefore, $x^p + a$ is reducible. □

5. Let $\sigma_m : \mathbb{Z} \to \mathbb{Z}_m$ be the natural reminder homomorphism sending $a$ to the remainder of $a$ when divided by $m$, for $a \in \mathbb{Z}$.

   (a) Show that the induced map $\overline{\sigma}_m : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ given by

   $$\overline{\sigma}_m(a_0 + a_1 x + \cdots + a_n x^n) = \sigma_m(a_0) + \sigma_m(a_1)x + \cdots + \sigma_m(a_n)x^n$$

   is a homomorphism from $\mathbb{Z}[x]$ onto $\mathbb{Z}_m[x]$.

   (b) Show that if $f(x) \in \mathbb{Z}[x]$ and $\overline{\sigma}_m(f(x))$ both have degree $n$ and $\overline{\sigma}_m(f(x))$ does not factor in $\mathbb{Z}_m[x]$ into two polynomials of degree less than $n$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

   (c) Use part (b) to show that $x^3 + 17x + 36$ is irreducible in $\mathbb{Q}[x]$.

   *Proof.* (a) In general, let $\phi : R \to R'$ be a ring homomorphism, then $\overline{\phi} : R[x] \to R'[x]$ given by $\overline{\phi}(\sum_{i=0}^n r_i x^i) = \sum_{i=0}^n \phi(r_i)x^i$ for $n \in \mathbb{Z}_{\geq 0}, r_0, ..., r_n \in R$ is a ring homomorphism. We prove this more general statement, and (a) will follow by taking $\phi$ as $\sigma_m : \mathbb{Z} \to \mathbb{Z}_m$.

   Since $\phi$ is a ring homomorphism, $\phi(1_R) = 1_{R'}$. Then $\overline{\phi}(1_{R[x]}) = \overline{\phi}(1_R) = \phi(1_R) = 1_{R'} = 1_{R'[x]}$.

   Let $f = \sum\limits_{i=0}^{N} a_i x^i, g = \sum\limits_{i=0}^{N} b_i x^i$, where $N$ is some large enough integer. Then $f + g = \sum\limits_{i=0}^{N}(a_i + b_i)x^i$. Then $\phi(f + g) = \sum\limits_{i=0}^{N} \phi(a_i + b_i)x^i = \sum\limits_{i=0}^{N}(\phi(a_i) + \phi(b_i))x^i = \sum\limits_{i=0}^{N} \phi(a_i)x^i + \sum\limits_{i=0}^{N} \phi(b_i)x^i = \phi(f) + \phi(g)$.

   On the other hand, $fg = \sum\limits_{k=0}^{2N}(\sum\limits_{i+j=k} a_i b_j)x^k$. Then $\phi(fg) = \sum\limits_{k=0}^{2N} \phi(\sum\limits_{i+j=k} a_i b_j)x^k = \sum\limits_{k=0}^{2N}(\sum\limits_{i+j=k} \phi(a_i)\phi(b_j))x^k = (\sum\limits_{i=0}^{N} \phi(a_i)x^i)(\sum\limits_{i=0}^{N} \phi(b_i)x^i) = \phi(f)\phi(g)$.

   Then $\overline{\phi}$ is a ring homomorphism.

   (b) Suppose $f(x) \in \mathbb{Z}[x]$ and $\overline{\sigma}_m(f(x))$ both have degree $n$ and $\overline{\sigma}_m(f(x))$ does not factor in $\mathbb{Z}_m[x]$ into two polynomials of degree less than $n$.

   Suppose $f(x)$ is reducible in $\mathbb{Q}[x]$, then $f$ is reducible into polynomials of lower degrees in $\mathbb{Z}[x]$ by Gauss lemma. That is, $f = gh$ for some $g, h \in \mathbb{Z}[x]$ with $0 < \deg(g), \deg(h) < \deg(f)$.

   Then $\sigma_m(f) = \sigma_m(g)\sigma_m(h)$ by (a). Note that $\deg(\sigma_m(g)) \leq \deg(g) < \deg(f) = \deg(\sigma_m(f))$, and $\deg(\sigma_m(h)) \leq \deg(h) < \deg(f) = \deg(\sigma_m(f))$. This contradicts the assumption on the irreducibility of $\sigma_m(f)$.

(c) Let $f = x^3 + 17x + 36$. Then $\sigma_5(f) = x^3 + 2x + 1 \in \mathbb{Z}_5[x]$. Note that $\sigma_5(f)(0) = 1, \sigma_5(f)(1) = 4, \sigma_5(f)(2) = 3, \sigma_5(f)(3) = 4, \sigma_5(f)(4) = 3$. Then $\sigma_5(f)$ has no root in $\mathbb{Z}_5$. Since $\deg(\sigma_5(f)) = \deg(f) = 3$, $\sigma_5(f)$ is irreducible in $\mathbb{Z}_5[x]$. By (b), $f = x^3 + 17x + 36$ is irreducible in $\mathbb{Q}[x]$.

□

6. Let $\phi : R \to R'$ be a ring homomorphism and let $N$ be an ideal of $R$.

(a) Show that $\phi[N]$ is an ideal of $\phi[R]$.

(b) Given an example to show that $\phi[N]$ need not be an ideal of $R'$.

(c) Let $N'$ be an ideal either of $\phi[R]$ or of $R'$. Show that $\phi^{-1}[N']$ is an ideal of $R$.

*Proof.* (a) This is Property 5 of Proposition 8.1 in Tutorial 8. We copy the proof here.

Since $N$ is an ideal of $R$, it is an additive subgroup of $R$, and for $r \in R$, $n \in N$, $rn, nr \in N$. Then $\phi(N)$ is an additive subgroup of $\phi(R)$ and for $x \in \phi(R)$, $y \in \phi(N)$, there exists $r \in R, n \in N$ such that $\phi(r) = x, \phi(n) = y$. Then $xy = \phi(r)\phi(n) = \phi(rn) \in \phi(N)$, and $yx = \phi(n)\phi(r) = \phi(nr) \in \phi(N)$. Then, $\phi(N)$ is an ideal of $\phi(R)$.

(b) Let $R = \mathbb{Z}, R' = \mathbb{Q}$, and $\phi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. Let $N = 2\mathbb{Z}$. Then $N$ is an ideal of $R$, while $\phi(N) = 2\mathbb{Z}$ is not an ideal of $R'$, because the only ideals of $R'$ are $0$ and $R'$.

(c) This is Property 6 of Proposition 8.1 in Tutorial 8. We copy the proof here.

If $N'$ is an ideal of $R'$, then it is also an ideal of $\phi(R)$. So we suppose $N'$ is an ideal of $\phi(R)$. Then $\phi^{-1}(N')$ is an additive subgroup of $R$. Let $r \in R, n \in \phi^{-1}(N')$, $\phi(r) \in \phi(R)$ and $\phi(n) \in N'$. Then $\phi(rn) = \phi(r)\phi(n) \in N'$, $\phi(nr) = \phi(n)\phi(r) \in N'$. Then $rn, nr \in \phi^{-1}(N')$. It follows that $\phi^{-1}(N')$ is an ideal of $R$.

□

**Optional Part**

1. Let $F$ be a field. An element $\phi$ of $F^F$ is a **polynomial function on** $F$, if there exists $f(x) \in F[x]$ such that $\phi(a) = f(a)$ for all $a \in F$.

   (a) Show that the set $P_F$ of all polynomial functions on $F$ forms a subring of $F^F$.

   (b) Give an example to show that the ring $P_F$ is not necessarily isomorphic to $F[x]$.

   *Proof.* (a) Let $F^F$ be the ring of functions from $F$ to itself, with addition and multiplication be defined by $(f+g)(x) := f(x)+g(x)$ for all $x \in F$ and $(f \cdot g)(x) = f(x)g(x)$ for all $x$. We take it for granted that $F^F$ forms a ring under these operations.

   Let $\alpha : F[x] \to F^F$ be the map such that $\alpha(f)(a) = f(a) = \mathrm{ev}_a(f)$ for any $a \in F$. Then $\alpha$ maps a polynomial to its corresponding function.

   Note that $\alpha(1) = 1 = 1_{F^F}$, the function that sends $F$ to 1. For $f, g \in F[x]$, for any $a \in F$, $\alpha(f+g)(a) = ev_a(f+g) = ev_a(f) + ev_a(g) = \alpha(f)(a) + \alpha(g)(a) = (\alpha(f)+\alpha(g))(a)$. Then $\alpha(f+g) = \alpha(f)+\alpha(g)$. Similarly, $\alpha(f \cdot g)(a) = ev_a(f \cdot g) = ev_a(f) \cdot ev_a(g) = \alpha(f)(a) \cdot \alpha(g)(a) = (\alpha(f) \cdot \alpha(g))(a)$. Then $\alpha(f \cdot g) = \alpha(f) \cdot \alpha(g)$. Therefore, $\alpha$ is a ring homomorphism.

   Note that $P_F = \alpha(F[x])$. Therefore, $P_F$ is a subring of $F^F$.

   (b) See question 2.

   $\square$

   **Remark.** On the other hand, when $F$ is an infinite field, $\alpha$ is injective, and thus $P_F \simeq F[x]$. The reason is that if $\alpha(f) = 0$, then $f(a) = 0$ for any $a \in F$. When $|F| = \infty$. This implies $f = 0$ by the root theorem.

2. Give an example to show that, when $F$ is a finite field, $P_F$ and $F[x]$ do not even have the same number of elements.

   *Proof.* Let $F$ be a finite field with $|F| = q$. Then $|P_F| \leq |F^F| = q^q < \infty$, while $|F[x]| = \infty$. $\square$

3. Let $F$ be a field of characteristic zero and let $D$ be the formal polynomial differentiation map, i.e.

$$D(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) := a_1 + 2 \cdot a_2 x + \cdots + n \cdot a_n x^{n-1}.$$

   (a) Show that $D : F[x] \to F[x]$ is a group homomorphism from $(F[x], +)$ into itself. Is $D$ a ring homomorphism?

   (b) Find the kernel of $D$.

   (c) Find the image of $F[x]$ under $D$.

   *Proof.* Let $F$ be a field of characteristic zero and let $D$ be the formal polynomial differentiation map.

(a) Let $a_0, ..., a_n, b_0, ..., b_n \in F$. Note that $D(\sum_{i=0}^n a_i x^i) = \sum_{i=1}^n i a_i x^{i-1}$. Then $D(\sum_{i=0}^n a_i x^i + \sum_{i=0}^n b_i x^i) = D(\sum_{i=0}^n (a_i + b_i) x^i) = \sum_{i=0}^n i(a_i+b_i)x^{i-1} = \sum_{i=1}^n i a_i x^{i-1} + \sum_{i=1}^n i b_i x^{i-1} = D(\sum_{i=1}^n a_i x^i) + D(\sum_{i=1}^n b_i x^i)$.
Note that however $D(1) = 0$, so it is not a ring homomorphism.

(b) Let $f = \sum_{i=0}^n a_i x^i$. Suppose $D(f) = 0$. Then $i a_i = 0$ for any $i > 0$. Since $\text{char}(F) = 0$, $a_i = 0$ for $i > 0$. Then $f = a_0$. Conversely, $D(a_0) = 0$. Therefore, $\ker(D) = F$.

(c) Since $\text{char}(F) = 0$, each $i \in \mathbb{Z}_{>0}$ is invertible in $F$. For any $f = \sum_{i=0}^n a_i x^i \in F[x]$, let $g = \sum_{i=0}^n \frac{a_i x^{i+1}}{i+1}$. Then $D(g) = f$. Therefore $D$ is surjective, that is, the image of $F[x]$ under $D$ is $F[x]$.

□

4. Let $A$ and $B$ be ideals of a ring $R$. The **product** $AB$ **of** $A$ **and** $B$ is defined by

$$AB = \left\{ \sum_{i=1}^n a_i b_i : a_i \in A, b_i \in B, n \in \mathbb{Z}^+ \right\}.$$

(a) Show that $AB$ is an ideal in $R$.

(b) Show that $AB \subseteq (A \cap B)$.

*Proof.* (a) Let $\sum_{i=1}^n a_i b_i \in AB$, then its additive inverse $-\sum_{i=1}^n a_i b_i = \sum_{i=1}^n (-a_i) b_i \in AB$, and it is clear that $AB$ is closed under addition. If $r \in R$ is any element, since $A, B$ are ideals, we have $r \sum_{i=1}^n a_i b_i = \sum_{i=1}^n (r a_i) b_i \in AB$ as $r a_i \in A$ and $(\sum_{i=1}^n a_i b_i) r = \sum_{i=1}^n a_i (b_i r) \in AB$ as $b_i r \in B$.

(b) Since $A, B$ are ideals, $a_i b_i \in A \cap B$ for any $\sum_{i=1}^n a_i b_i \in AB$, therefore so is their sum.

□

5. Let $A$ and $B$ be ideals of a *commutative* ring $R$. The **quotient** $A : B$ **of** $A$ **by** $B$ is defined by

$$A : B = \{ r \in R : rb \in A \text{ for all } b \in B \}.$$

Show that $A : B$ is an ideal of $R$.

*Proof.* Let $r, s \in A : B$, then $rb, sb \in A$ for all $b \in B$, therefore $(r+s)b, -rb \in A$ for all $b \in B$, since $A$ is an additive subgroup. Let $x \in R$, then $xrb \in A$ for any $b \in B$ since $A$ is an ideal and $rb \in A$. For commutative ring, we only have to check one side, therefore $A : B$ is indeed an ideal.

□

6. Let $R$ and $R'$ be rings and let $N$ and $N'$ be ideals of $R$ and $R'$, respectively. Let $\phi$ be a homomorphism of $R$ into $R'$. Show that $\phi$ induces a natural homomorphism $\phi_* : R/N \to R'/N'$ if $\phi[N] \subseteq N'$.

*Proof.* Let $R$ and $R'$ be rings and let $N$ and $N'$ be ideals of $R$ and $R'$, respectively. Let $\phi$ be a homomorphism of $R$ into $R'$. Suppose $\phi[N] \subseteq N'$. Let $\pi : R' \to R'/N'$ be the natural projection. Then $\psi := \pi \circ \phi : R \to R'/N'$ is a ring homomorphism. Now, $\psi(N) = \pi(\phi(N)) \subseteq \pi(N') = 0$. Then $\psi$ factors through $R/N$, that is, $\psi$ induces a natural homomorphism $\phi_* : R/N \to R'/N'$. $\square$