NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Kenny Sng, Lau Tze Siong

**MA3201 Algebra II**
AY 2008/2009 Semester 2

---

## Question 1

(a) True. Suppose that $J$ is an ideal of $S$. Let $x, y \in \phi^{-1}(J)$. Then, $\phi(x-y) = \phi(x) - \phi(y) \in J$ since both $\phi(x)$ and $\phi(y)$ are in $J$ and $J$ is an ideal of $S$. Thus, $x - y \in \phi^{-1}(J)$. For all $r \in R$, $\phi(rx) = \phi(r)\phi(x) \in J$ since $\phi(r) \in S$, $\phi(x) \in J$ and $J$ is an ideal of $S$. Hence, $\phi^{-1}(J)$ is an ideal of $R$.

(b) True. First we check that $\phi^{-1}(J) \neq R$. If $1_S \in J$, then for all $s \in S$, $s = 1_S s \in J$, and thus $J = S$, which is a contradiction to the fact that $J$ is a prime ideal of $S$. Hence, $1_S \notin J$, and since $\phi(1_S) = 1_R$, we conclude that $1_R \notin \phi^{-1}(J)$, and that $\phi^{-1}(J) \neq R$.

Suppose that $xy \in \phi^{-1}(J)$. Then, $\phi(xy) = \phi(x)\phi(y) \in J$, which implies that either $\phi(x) \in J$ or $\phi(y) \in J$, which means that either $x \in \phi^{-1}(J)$ or $y \in \phi^{-1}(J)$. Hence, $\phi^{-1}(J)$ is a prime ideal of $R$.

(c) False. Consider the inclusion map $\phi : \mathbb{Z} \to \mathbb{Q}$. In $\mathbb{Q}$, the zero ideal $\{0\}$ is the maximal ideal, but $\phi^{-1}(\{0\}) = \{0\} \in \mathbb{Z}$ is not a maximal ideal, as $2\mathbb{Z}$ is also an ideal of $\mathbb{Z}$, but $\{0\} \subset 2\mathbb{Z} \subsetneq \mathbb{Z}$.

## Question 2

(a) (i) (Note: A mistake was spotted in the question during the examination. The correct question should read: "*Show that $I$ is a non-zero maximal ideal of $R$ if and only if $I = (a)$ for some irreducible $a \in R$.*")

Let $I$ be a non-zero maximal ideal of $R$. Since $R$ is a principal ideal domain (PID), $I = (a)$ for some $a \in R$. Suppose that $a = st$ for some $s, t \in R$. Then, $s|a$, and thus $(a) \subseteq (s) \subseteq R$. Since $I$ is maximal, either $(r) = (s)$ or $(s) = R$. If $(s) = R$, then there exists an $s' \in R$ such that $ss' = 1_R$, which implies that $s$ is a unit. If $(r) = (s)$, then $r$ and $s$ are associates, which implies that $t$ is a unit. Hence, we conclude that either $s$ or $t$ is a unit, and thus $a$ is irreducible in $R$.

Suppose now that $I = (a)$ for some irreducible $a \in R$. Then, $a$ is non-zero and a non-unit, and hence $\{0\} \subsetneq (a) \subsetneq R$. Suppose for a contradiction that there exists an $s \in R$ such that $(a) \subsetneq (s) \subsetneq R$. Similarly, $s$ is also non-zero and a non-unit. Thus, $a = st$ for some $t \in R$, and since $a$ is irreducible and $s$ is a non-unit, it follows that $t$ is a unit of $R$. This implies that $a$ and $s$ are associates, and that $(r) = (s)$, which is a contradiction. Hence, $I$ is a non-zero maximal ideal of $R$.

(ii) Let $I$ be a non-zero prime ideal of $R$. Then, $I = (a)$ for some $a$ which is prime in $R$. Since $a$ is prime in a PID, $a$ is irreducible, and we conclude that $I$ is a non-zero maximal ideal of $R$ by (i). Hence, the only prime ideal which is not maximal is the zero ideal.

(b) (i) Let $h = \gcd(r_1, r_2)$ in $S$. Since $g = \gcd(r_1, r_2)$ in $R$, $g|r_1$ and $g|r_2$ in $R$, and hence $g|r_1$ and $g|r_2$ in $S$. Thus, $g|h$ in $S$ since $h = \gcd(r_1, r_2)$ in $S$.

$h|r_1$ and $h|r_2$ in $S$ implies that $r_1 = hs_1$ and $r_2 = hs_2$ for some $s_1, s_2 \in S$. Hence,

$$\begin{aligned} g &= ar_1 + br_2 \\ &= ahs_1 + bhs_2 \\ &= h(as_1 + bs_2), \end{aligned}$$

which implies that $h|g$ in $S$. Thus, $h$ and $g$ are associates in $S$, and $g = \gcd(r, s)$ in $s$.

(ii) No. Let $R = \mathbb{Z}[X]$, $S$ be the subring of $\mathbb{Q}[X]$ consisting of polynomials with integer constants. Let $r_1 = X^2$, $r_2 = 2X$. Then, in $R$, $\gcd(r_1, r_2) = X$. Suppose that $X$ is the greatest common divisor of $r_1$ and $r_2$ in $S$. Since $X^2 = (2X)(\frac{X}{2})$, $2X$ divides both $X^2$ and $2X$ in $S$, but $2X$ does not divide $X$ in $S$ since $\frac{1}{2} \notin S$, which is a contradiction.

**Question 3**

(a) Let $\sum r_i X^i \in R[X]$.If $\Phi$ is a ring homomorphism such that $\Phi(r) = \phi(r)$ for all $r \in R$ and $\Phi(X) = X$,

$$\begin{aligned} \Phi(\sum r_i X^i) &= \sum \Phi(r_i)\Phi(X^i) \\ &= \sum \phi(r_i)\Phi(X)^i \\ &= \sum \phi(r_i)X^i. \end{aligned}$$

Thus, the required ring homomorphism $\Phi : R[X] \to S[X]$ is defined by $\Phi(\sum r_i X^i) = \sum \phi(r_i)X^i$, and by the above discussion, $\Phi$ is unique.

(b) (i) The map $\psi$ is a unital ring homomorphism, and by $(a)$, there exists a unique ring homomorphism $\Psi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ defined by $\Psi(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \overline{a_i} X^i$ for all $\sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ such that $\Psi(r) = \psi(r) = \overline{r}$ for all $r \in \mathbb{Z}$ and $\Psi(X) = X$.

Suppose that $\sum_{i=0}^n \overline{a_i} X^i$ is irreducible in $\mathbb{Z}_p[X]$, and suppose for a contradiction that $f(X) = \sum_{i=0}^n a_i X^i$ is reducible in $\mathbb{Q}[X]$. If $\sum_{i=0}^n a_i X^i$ is reducible in $\mathbb{Q}[X]$, then it is reducible in $\mathbb{Z}[X]$, and thus there exists polynomials $g(X) = \sum_{i=0}^m b_i X_i$ and $h(X) = \sum_{i=0}^k c_i X_i$ in $\mathbb{Z}[X]$, $0 < m < n$, $0 < k < n$ such that $f(X) = g(X)h(X)$. Hence,

$$\begin{aligned} \Psi(f(X)) &= \sum_{i=0}^n \overline{a_i} X^i \\ &= (\sum_{i=0}^m \overline{b_i} X_i)(\sum_{i=0}^k \overline{c_i} X_i). \end{aligned}$$

Since $p$ does not divide $a_n$ in $\mathbb{Z}$, $\overline{a_n} \neq \overline{0}$ in $\mathbb{Z}_p$, and thus $\overline{b_m c_k} \neq \overline{0}$. Thus, $p$ does not divide $b_m c_k$ in $\mathbb{Z}$, which implies that $p$ does not divide $b_m$ and $p$ does not divide $c_k$. Consequently, both $\sum_{i=0}^m \overline{b_i} X_i$ and $\sum_{i=0}^k \overline{c_i} X_i$ are nonconstant polynomials in $\mathbb{Z}_p[X]$. For an integral domain $R$, the set of units of $R[X]$ coincide with the set of units of $R$. Hence, the set of units of $\mathbb{Z}_p[X]$ are the units of $\mathbb{Z}_p$, which are the non-zero elements of $\mathbb{Z}_p$ since $\mathbb{Z}_p$ is a field. Hence, both $\sum_{i=0}^m \overline{b_i} X_i$ and $\sum_{i=0}^k \overline{c_i} X_i$ are non-units in $\mathbb{Z}_p[X]$, which contradicts the fact that $\sum_{i=0}^n \overline{a_i} X^i$ is irreducible in $\mathbb{Z}_p[X]$.

(ii) No. Consider $f(X) = 2X^2 + 2 \in \mathbb{Z}[X]$, and consider $p = 3$. Then, we first show that $\overline{f(X)}$ is irreducible in $\mathbb{Z}_3[X]$. Suppose on the contrary that $\overline{f(X)} = \overline{g(X)}\overline{h(X)}$ where $\overline{g(X)} = \overline{a}X + \overline{b}$ and $\overline{h(X)} = \overline{c}X + \overline{d}$ are non-constant polynomials of degree 1. Hence, by comparing the powers of $X^2$, $\overline{ac} = \overline{2}$, and hence $\{\overline{a}, \overline{c}\} = \{\overline{1}, \overline{2}\}$. Without loss of generality, assume that $\overline{a} = 1$ and $\overline{c} = 2$. By comparing the coefficients of the other powers of $X$, we arrive at

$$\begin{aligned} \overline{d} + \overline{2b} &= 0 \\ \overline{bd} &= 2. \end{aligned}$$

Hence, by a similar reasoning, $\{\overline{b}, \overline{d}\} = \{\overline{1}, \overline{2}\}$, which is a contradiction to $\overline{d} + \overline{2b} = 0$. Hence, $\overline{f(X)}$ is irreducible in $\mathbb{Z}_3[X]$. However, $2X^2 + 2 = 2(X^2 + 1)$, and hence is not irreducible in $\mathbb{Z}[X]$.

(iii) No. Let $f(X) = X^2 + 1 \in \mathbb{Z}[X]$, which is irreducible in $\mathbb{Z}[X]$, but $X^2 + \overline{1} = (X + \overline{1})(X + \overline{1})$ in $\mathbb{Z}_2[X]$, and thus $\overline{f(X)}$ is not irreducible in $\mathbb{Z}_2[X]$.

**Question 4**

(i) Suppose that $N$ and $M/N$ are finitely generated. Hence, there exists $k, l \in \mathbb{Z}^+$, $n_1, n_2, ..., n_k \in N$, $m_1 + N, m_2 + N, ..., m_l + N \in M/N$ such that $N = Rn_1 + ... + Rn_k$ and $M/N = R(m_1 + N) + ... + R(m_l + N)$.

Hence, for all $\alpha \in M$,

$$\begin{aligned} & \alpha + N = \sum_{i=1}^{l} r_i(m_i + N) \quad \text{for some } r_i \in R,\ i = 1, 2, ..., l \\ \Rightarrow \quad & \alpha + N = (\sum_{i=1}^{l} r_i m_i) + N \\ \Rightarrow \quad & \alpha - \sum_{i=1}^{l} r_i m_i \in N \\ \Rightarrow \quad & \alpha - \sum_{i=1}^{l} r_i m_i = \sum_{j=1}^{k} s_j n_j \quad \text{for some } s_j \in R,\ j = 1, 2, ..., k \\ \Rightarrow \quad & \alpha = \sum_{i=1}^{l} r_i m_i + \sum_{j=1}^{k} s_j n_j, \end{aligned}$$

which implies that $M$ is finitely generated.

(ii) Let $R = M = \{a_0 + a_1X + ... + a_nX^n | a_0 \in \mathbb{Z}, a_1, a_2, ..., a_n \in \mathbb{Q}, n \in \mathbb{Z}_{\geq 0}\}$. and $N = \{a_1X + ... + a_nX^n | a_1, a_2, ..., a_n \in \mathbb{Q}, n \in \mathbb{Z}_{\geq 0}\}$. Then, $N$ is an ideal of $M$, and thus can be viewed as a $R-$submodule of $M$. Suppose that $N$ is finitely generated as an $R-$ module. Hence, $N = Rf_1 + Rf_2 + ... + Rf_k$, where $f_1, f_2, ..., f_k \in N$. Hence, the coefficient of $X$ of any polynomial from $N$, which is a rational number, will have to be of the form $n_1a_1 + ... + n_ka_k$, where $n_1, ..., n_k \in \mathbb{Z}$, $a_i$ is the coefficient of $X$ in $f_i$ for $i = 1, 2, ..., k$. Hence, such coefficients of $X$ can only have denominators dividing the lowest common multiple of the denominators of the $a_i$'s, but obviously not all rational numbers are of this form. Hence, $N$ cannot be finitely generated.

(iii) True. Since $M$ is a finitely generated $R-$module, there exists a surjective $R-$module homomorphism $\phi : F \to M$ where $F$ is free of finite rank. Then, $q \circ \phi : F \to M/N$ is also a surjective $R-$module homomorphism, where $q : M \to M/N$ is the quotient module homomorphism. Hence, $M/N$ is also finitely generated.