NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Lau Tze Siong

MA3201 Algebra II
AY 2006/2007 Sem 2

Question 1

(a) (i) f is a ring homomorphism if and only if for all $a, b \in R$, $f(a +_R b) = f(a) +_S f(b)$ and $f(a \times_R b) = f(a) \times_S f(b)$.

(ii) $\ker(f) = \{a \in R \mid f(a) = 0_S\}$.

(b) (i) For all $r \in \ker(\phi)$, one has $\phi(r) = 0_S$. Hence $\psi(r) = \theta \circ \phi(r) = \theta(0_S) = 0_T$. Therefore $r \in \ker(\psi)$. Hence $\ker(\phi) \subseteq \ker(\psi)$

(ii) **Existence**
Since ϕ is surjective, for all $s \in S$ there exists $r \in R$ such that $\phi(r) = s$. Hence, define $\theta : S \to T$ such that $\theta(s) = \psi(r)$ where $\phi(r) = s$. Claim: θ is a well-defined homomorphism.
Proof:
Fix $s \in S$ Let $r_1, r_2 \in R$ such that $\phi(r_1) = \phi(r_2) = s$. Hence $r_1 - r_2 \in \ker(\phi) \subseteq \ker(\psi)$. Therefore $\psi(r_1 - r_2) = 0_T$. Hence we have $\psi(r_1) = \psi(r_2)$.
Therefore θ is a well-defined function.
Let $s_1, s_2 \in S$ and $r_1, r_2 \in R$ such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$.

$$\begin{aligned} \theta(s_1 + s_2) &= \psi(r_1 + r_2) \\ &= \psi(r_1) + \psi(r_2) \\ &= \theta(s_1) + \theta(s_2) \end{aligned}$$

$$\begin{aligned} \theta(s_1 s_2) &= \psi(r_1 r_2) \\ &= \psi(r_1)\psi(r_2) \\ &= \theta(s_1)\theta(s_2) \end{aligned}$$

Hence θ respects both addition and multiplication.
Therefore θ is a homomorphism. □
Since for all $s \in S$, $\theta \circ \phi(s) = \theta(r)$ such that $r = \phi(s)$. $\theta(r) = \psi(s)$ by definition of θ. Hence there exist a $\theta : S \to T$ such that $\theta \circ \phi = \psi$.
Uniqueness
Suppose there exists $\theta_1, \theta_2 : S \to T$ such that $\theta_1 \circ \phi = \theta_2 \circ \phi = \psi$. Since ϕ is surjective, for all $s \in S$, $s = \phi(r)$ for some $r \in R$. $\theta_1(s) = \theta_1 \circ \phi(r) = \psi(r)$ and $\theta_2 \circ \phi(r) = \psi(r)$. Hence we have $\theta_1 = \theta_2$. □

Question 2

(a) (i) An ideal I is prime if and only if for any $r_1, r_2 \in R$ such that $r_1 r_2 \in I$, one has $r_1 \in I$ or $r_2 \in I$.

(ii) An ideal I is maximal in R if and only if I is not R and for any ideal J such that $J \supsetneq I$, $J = R$.

(b) (i) An element $a \in R$ is prime if and only if a is non-zero non-unit element and for any $b, c \in R$ such that $a \mid bc$ then $a \mid b$ or $a \mid c$.

(ii) An element $a \in R$ is irreducible if and only if it is non-unit and for any $b, c \in R$ such that $bc = a$ then either b is unit or a is unit.

(c) (i) Claim: I is a prime ideal.
Proof:
Let $p(X), q(X) \in R[X]$ such that $pq \in I$. Hence we have $p(X)q(X) = f(X)a(X)$ for some $a(X) \in R[X]$. Since R is a UFD, $R[X]$ is a UFD. Hence $f(X)$ is prime. Since $f(X) \mid p(X)q(X)$, $f(X) \mid p(X)$ or $f(X) \mid q(X)$ which is equivalent to saying either $p(X) \in I$ or $q(X) \in I$. Hence I is a prime ideal. $\square$
Claim: J is a maximal ideal.
Proof:
Since F is field, $F[X]$ is a Euclidean Domain. Now suppose K is a ideal such that $K \supsetneq J$. Then there exist $p(X) \in K \backslash J$. Hence $f(X) \nmid p(X)$. Since $f(X)$ is irreducible, we have $\gcd(f(X), p(X)) = 1$. Hence there exist $\alpha(X), \beta(X) \in F[X]$ such that $\alpha(X)f(X) + \beta(X)p(X) = 1$. Therefore $1 \in J$. Hence $J = F[X]$. Hence I is maximal. $\square$

(ii) Let $R = \mathbb{Z}[Y]$.Since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[Y]$ is a UFD. Since R is a UFD, $R[X]$ is a UFD. Since X is irreducible, $\langle X \rangle$ is a prime ideal. But $\langle X \rangle \subsetneq \langle X, Y \rangle \subsetneq< R[X]$. Hence $\langle X \rangle$ is prime but not maximal.

Question 3

(a) (i) A Euclidean Function is a map $\phi : R \backslash 0 \to \mathbb{Z}_+$ such that for any $a, b \in R\backslash\{0\}$, $\phi(ab) \geq \max(\phi(a), \phi(b))$ and there exists q, r such that $a = qb + r$ where $\phi(r) < \phi(b)$ or $r = 0$.

(ii) A Euclidean Domain is a Integral Domain which a Euclidean Function can be defined on.

(b) Let $\phi(r) = 1$ for all $r \in F\backslash\{0\}$. This is a Euclidean function since for any $a, b \in R\backslash\{0\}$, $\phi(ab) \geq \max(\phi(a), \phi(b))$. The second condition is satisfied trivially since all non-zero elements in F are units hence are associates.
Since a field F is in particular a Integral Domain and we can define a Euclidean Function for all fields.
A field is a Euclidean Domain. $\square$

(c) Define

$$N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_+$$

such that

$$N(a + b\sqrt{2}) = |a^2 - 2b^2|$$

. For any $a + b\sqrt{2}, p + q\sqrt{2} \in \mathbb{Z}\sqrt{2}$, we need to find $\alpha, r \in \mathbb{Z}\sqrt{2}$ such that

$$a + b\sqrt{2} = \alpha(p + q\sqrt{2}) + r$$

and $N(r) < N(p + q\sqrt{2})$. Rearranging the equation we have

$$\frac{r}{p + q\sqrt{2}} = \frac{a + b\sqrt{2}}{p + q\sqrt{2}} - \alpha$$

. Since $\mathbb{Q}\sqrt{2}$ is a field, $\frac{a+b\sqrt{2}}{p+q\sqrt{2}} = m + n\sqrt{2}$ for some $m, n \in \mathbb{Q}$.

Hence we need to find $\alpha \in \mathbb{Z}\sqrt{2}$ such that $N(m + n\sqrt{2} - \alpha) < 1$.

To do this, note for any $m, n \in \mathbb{Q}$, there exist $x, y \in \mathbb{Z}$ such that $(m - x) \leq \frac{1}{2}$ and $(n - y) \leq \frac{1}{2}$. Therefore we let $\alpha = x + y\sqrt{2}$ such that the previous two inequalities are satisfied. Hence $N(m + n\sqrt{2} - \alpha) = |(m - x)^2 - 2(n - y)^2| < \frac{1}{4} + (2)\frac{1}{4} < 1$.
Since $m + n\sqrt{2} - \alpha = \frac{r}{p+q\sqrt{2}}$, we have $N\left(\frac{r}{p+q\sqrt{2}}\right) < 1$. This gives us $N(r) < N(p + q\sqrt{2})$.
Hence we have found $\alpha, r \in \mathbb{Z}\sqrt{2}$ such that $a + b\sqrt{2} = \alpha(p + q\sqrt{2}) + r$ and $N(r) < N(p + q\sqrt{2})$. $\square$

Question 4

(a) The sum $N_1 + N_2 + n_3 + ... + N_r$ is direct if and only if for any $n_i \in M_i$ and $k_i \in R$ for $i = 1, ..., r$. One has $\sum_{i=1}^{r} k_i n_i = 0_M$ if and only if $k_i = 0_R$ for all $i = 1, ..., r$.

(b) (i) For $i = 1, ..., r$, let $k_i \in R$ and $v_i \in V_i$ such that

$$\sum_{i=1}^{r} k_i v_i = 0_M$$

. Since each $V_i \subseteq U_i$ for $i = 1, ..., r$, we have $v_i \in U_i$ for all $i = 1, ..., r$. Also, since $U_1 + U_2 + U_3 + ... + U_r$ is direct,$k_i = 0_R$ for $i = 1, ...r$.

(ii) Define the map

$$\phi : M \to (U_1/V_1) \times (U_2/V_2) \times (U_3/V_3) \times ... \times (U_r/V_r)$$

such that

$$u_1 + u_2 + u_3 + ... + u_r \mapsto (u_1 + V_1, u_2 + V_2, u_3 + V_3, ..., u_r + V_r)$$

This map is will defined since

$$M = U_1 \bigoplus U_2 \bigoplus U_3 \bigoplus ... \bigoplus U_r$$

,for $u_i, u_i' \in U_i$,

$$u_1 + u_2 + u_3 + ... + u_r = u_1' + u_2' + u_3' + ... + u_r'$$

if and only if $u_i = u_i'$ for all $i = 1, ..., r$.

Claim: ϕ is a surjective homomorphism with $\ker(\phi) = V$.
Proof:
For $m_1, m_2 \in M$ and $\alpha \in R$, we write $m_1 = \sum_{i=1}^{r} u_i$ and $m_2 = \sum_{i=1}^{r} u_i'$ such that $u_i, u_i' \in U_i$.

$$\begin{aligned}
\phi(m_1 + \alpha m_2) &= \phi(\sum_{i=1}^{r} u_i + \alpha \sum_{i=1}^{r} u_i') \\
&= \phi(\sum_{i=1}^{r} (u_i + \alpha u_i')) \\
&= (u_1 + \alpha + u_1' + V, u_2 + \alpha + u_2' + V, u_3 + \alpha + u_3' + V, ..., u_r + \alpha + u_r' + V) \\
&= (u_1 + V, u_2 + V, u_3 + V, ..., u_r + V) + \alpha(u_1' + V, u_2' + V, u_3' + V, ..., u_r' + V) \\
&= \phi(\sum_{i=1}^{r} u_i) + \alpha\phi(\sum_{i=1}^{r} u_i') \\
&= \phi(m_1) + \alpha\phi(m_2)
\end{aligned}$$

. Therefore ϕ is a homomorphism.

ϕ is surjective since for any $(u_1+V, u_2+V, u_3+V, ..., u_r+V) \in (U_1/V_1)\times(U_2/V_2)\times(U_3/V_3)\times ... \times(U_r/V_r)$, one has $\phi(u_1+u_2+u_3+....+u_r) = (u_1+V, u_2+V, u_3+V, ..., u_r+V)$.

For any $u_1+u_2+u_3+...+u_r \in \ker(\phi)$, $\phi(u_1+u_2+u_3+...+u_r) = 0$ if and only if , $(u_1+V, u_2+V, u_3+V, ..., u_r+V) = 0$. If and only if $u_i \in V_i$ for $i = 1, ..., r$. If and only if $u_1+u_2+u_3+...+u_r \in V$ (Since $V_1+V_2+...+V_r$ is direct).
Therefore ϕ is a surjective homomorphism with $\ker(\phi) = V$. $\square$

By First Isomorphism Theorem, we have $M/V \cong (U_1/V_1)\times(U_2/V_2)\times(U_3/V_3)\times...\times(U_r/V_r)$

Question 5

(a) Suppose $n \neq 0$ and n is composite. Hence $m = pq$ where p is prime and $q \in \mathbb{N}_{>1}$. Let $a = p \cdot 1$ p-times. Since $n > p$, $a \neq 0$. Similarly let $b = q{\cdot}1$ q-times. Since $n > q$, $b \neq 0$. But $ab = 1{+}1{+}1{+}...{+}1$ $pq = m$-times. Hence $ab = 0$. Therefore a is a zero-divisor of R. Hence R has at least 1 zero-divisor.

(b) (i) Since ϕ is a unitary ring homomorphism,$\phi(1_R) = 1_S$. Define the additive cyclic group G generate by 1_S. Therefore $o(1_S) = m$. Since $n \cdot 1_S = \phi(n \cdot 1_R) = \phi(0_R) = 0_S$. Hence $m \mid n$. Therefore $ma = n$ for some $a \in \mathbb{Z}$.

(ii) If R has no zero-divisor and $n > 0$, then n is prime. Since $1 \neq 0$, characteristic of S $m \neq 1$. Since n is prime, $n = ma$ and $m \neq 1$, one has $m = n$. $\square$