NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Lau Tze Siong

MA3201 Algebra II
AY 2007/2008 Sem 2

Question 1

(a) False.
$\mathbb{Z}$ is a integral domain but $\mathbb{Z} \times \mathbb{Z}$ is not a integral domain since $(1,0) * (0,1) = (0,0)$.

(b) True.
Since n is prime if and only if $n\mathbb{Z}$ is a prime ideal. Since $\mathbb{Z}$ is a PID , $n\mathbb{Z}$ is a maximal ideal. Hence n is prime if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field. Since $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$, n is prime if and only if $\mathbb{Z}_n$ is a field.

(c) False.
Let R=$\mathbb{Z}_6$. $3x+3$ is a zero-divisor in $R[x]$ since $(3x+3).(2) = 0$ but $3x+3 \notin R$.

(d) True.
Suppose $\{q_1, q_2, q_3, ..., q_n\}$ is the finite set of generaters that generate $\mathbb{Q}$. We may assume that $q_i = \frac{a_i}{b_i}$ such that $\gcd(a_i, b_i) = 1$. Let $\{p_1, p_2, ..., p_m\}$ be the list of prime factors of $\{b_1, b_2, ..., b_n\}$, note that this list is finite since there are only finitely many b_i. Since there are infinitely many primes, we can choose p_{m+1} such that $p_{m+1} \notin \{p_1, p_2, ..., p_m\}$.
Claim: $\{q_1, q_2, .., q_n\}$ does not generate $\frac{1}{p_{m+1}}$.
Proof: Suppose not. There exist $k_1, k_2, ..., k_n$ such that $\sum_{i=1}^{n} k_i \frac{a_i}{b_i} = \frac{1}{p_{m+1}}$.
Hence we have $p_{m+1}\left(\sum_{i=1}^{n} a_i b_1 b_2 b_3 ... \hat{b_i} ... b_n\right) = b_1 b_2 b_3 ... b_n$. Hence $p_{m+1} \mid b_1 b_2 b_3 ... b_n$. Therefore we have $p_{m+1} \mid b_i$ for some $i \in \{1, ..., n\}$(Contradiction, since p_{m+1} is not a prime factor of any of b_i!).

(e) False.
Since $\mathbb{Z}_4$ is a free module over $\mathbb{Z}_4$. But the submodule $\{0,2\}$ over $\mathbb{Z}_4$ is not free. Since the cardinality of $\mathbb{Z}_4^n$ is 4^n and is never equals to the cardinality of $\{0,2\}$, it cannot be isomorphic to $(\mathbb{Z}_4)^n$ for all $n \in \mathbb{Z}$.

Question 2

Let I be an ideal in S. Since ϕ is surjective, $\phi^{-1}(S)$ is a ideal in R. Since R is a PID, $\phi^{-1}(S) =< j >$. Therefore for all $x \in I$, $x = \phi(r)$ for some $r \in < j >$. Since $r \in < j >$, $r = jy$ for some $y \in R$.Hence for all $x \in I$, $x = \phi(jy) = \phi(j)\phi(y)$ for some $y \in R$. Therefore I is a principal ideal generated by $\phi(j)$.
S need not be a principal ideal domain since it may not be a integral domain. An example would be $R = \mathbb{Z}$ and $S = \mathbb{Z}_4$. Where ϕ maps $x \in \mathbb{Z}$ onto its equivalent class modulo 4. It is easy to check that this map is surjective and Z is a principal ideals domain. However, $\mathbb{Z}_4$ is not a integral domain, hence not a principal ideal domain.

Question 3

Suppose $x^2 + y^3$ is reducible, then it can be expressed as a product of 2 non-units in $\mathbb{Q}[x, y] = (\mathbb{Q}[y])\,[x]$.

Case 1)
$x^2 + y^3 = (fx^2 + g)(h)$ where $f, g, h \in \mathbb{Q}[y]$ such that $\deg(h) \geq 1$. Comparing coefficients of x^2, we have $fh = 1$. Therefore $\deg(h) = 0$(Contradiction!).

Case 2)
$x^2+y^3 = (fx+g)(hx+k)$, where $f, g, h, k \in \mathbb{Q}[y]$. Comparing the coefficients of x^2 we have $fh = 1$, since the units of $\mathbb{Q}[x]$ are exactly the units of Q, $f, h \in \mathbb{Q}$. We may assume that $f = j = 1$, therefore $x^2 + y^3 = (x + g)(x + k)$. Comparing coefficients of x and x^0 we have $g = -k$ and $gk = y^3$ respectively. Solving this two equations gives us, $-k^2 = y^3$(Contradiction, since the degree of k^2 is always even but the degree of y^3 is odd!).

Hence $x^3 + y^3$ is not reducible in $\mathbb{Q}[x, y]$. $\square$

Question 4

(a) Claim: If $b' \neq 0$ then $b + b' \neq b$
Proof:
Suppose not the $b + b' = b$ then we have $b' = 0$ which is a contradiction! $\square$
Claim:R has no zero divisors.
Proof:
Suppose R has a left zero divisor a then there exist $b' \in R\backslash\{0\}$ such that $ab' = 0$,in particular $ab'a = 0$. By assumption, since $a \in R\backslash\{0\}$,there exist a unique b such that $aba = a$ (Note that $b \neq b'$ since $aba \neq 0$). Hence we have $aba+ab'a = a+0 = a$. Therefore $a(b+b')a = a$(Contradiction! Since $b \neq b + b'$). The same conclusion can be drawn from assuming R has a right zero divisor. Hence R has no zero divisors.

(b) Fix $a \in R\backslash\{0\}$, then there exist a unique b such that $a = aba$. For any $r \in R\backslash\{0\}$, since $ar - ar = 0$ and $a = aba$, we have $ar - abar = 0$. Hence $a\,(r - (ba)r) = 0$. Since $a \neq \backslash\{0\}$ and R has no zero divisors, one has $r - (ba)r = 0$. Therefore $r = (ba)r$ for any $r \in R$.
Similarly for any $r \in R\backslash\{0\}$, $r - (ba)r = 0$. Therefore $r^2 - r(ba)r = 0$. Factorizing, we obtain $(r - r(ba))r = 0$. Since $r \neq 0$ and R has no zero divisors, $r = r(ba)$.

Claim: ba is the unique element in R such that $(ba)r = r = r(ba)$ for all $r \in R$.
Proof:
Suppose there exist k such that $kr = r = rk$ for all $r \in R$ in particular $r \in R\backslash\{0\}$, then we have $kr = r = (ba)r$. Therefore $(k - ba)r = 0$. Since $r \neq 0$, we have $k = ba$. $\square$
Hence ba is the unique element such that $(ba)r = r = r(ba)$ for all $r \in R$. Therefore ba is the identity in R. Since R is a ring with identity without zero divisors, R is a division ring.

Question 5

(a) Suppose $a_1+a_2 \in I_1\cup I_2$, then $a_1+a_2 \in I_1$ or $a_1+a_2 \in I_2$. If $a_1+a_2 \in I_1$ then $a_1+a_2-a_1 = a_2 \in I_1$ which contradicts $a_2 \notin I_1$. Similarly, if $a_1 + a_2 \in I_2$ then $a_1 + a_2 - a_2 = a_1 \in I_2$ which contradicts $a_1 \notin I_2$.
Hence $a_1 + a_2 \notin I_1 \cup I_2$.

Claim: If $I_1 \subseteq I_2$ or $I_2 \subseteq I_1$ then $I_1 \cup I_2$ is an ideal.
Proof:
WLOG suppose $I_1 \subseteq I_2$ then $I_1 \cup I_2 = I_2$. Hence $I_1 \cup I_2$ is an ideal. $\square$

Claim: If $I_1 \cup I_2$ is a ideal, then either $I_1 \subseteq I_2$ or $I_2 \subseteq I_1$.
Proof:
By previous part, one of $I_1 \backslash I_2$ or $a_2 \in I_2 \backslash I_2$ must be empty. If not we can choose $a_1 \in I_1 \backslash I_2$ and $a_2 \in I_2 \backslash I_1$ but $a_1 + a_2 \notin I_1 \cup I_2$. WLOG suppose $I_1 \backslash I_2$ is empty, then $I_1 \subseteq I_2$. $\square$

Hence $I_1 \subseteq I_2$ or $I_2 \subseteq I_1$ if and only if $I_1 \cup I_2$ is an ideal.

(b) Claim: $a_2 a_3 a_4 ... a_n \notin P_1$
Proof:
Suppose not. Since P_1 is a prime ideal. $a_2 a_3 a_4 .. a_n \in P_1$ implies $a_i \in P_1$ for some $i \in \{2, 3, 4, 5, ..., n\}$ which is a contradiction! $\square$

Claim:$a_1 + a_2 a_3 ... a_n \notin \bigcup_{i=1}^{n} P_i$.
Proof:
Since for all $j \in \{2, ..., n\}$, $a_1 \in P_1 \backslash P_j$ and $a_2 a_3 ... a_n \in P_j \backslash P_1$, we have $a_1 + a_2 a_3 ... a_n \notin P_1 \cup P_j$ for all $j \in \{2, 3, ..., n\}$. Therefore $a_1 + a_2 a_3 ... a_n \notin \bigcup_{i=1}^{n} P_i$. $\square$

Claim: If I is an ideal such that $I \subseteq \bigcup_{i=1}^{n} P_i$ then $I \subseteq P_i$ for some $i = 1, ..., n$.
Proof:
Suppose not. Then there exist a collection of P_{m_α} ,$\alpha = 1, .., q$ such that $I \subseteq \bigcup_{i=1}^{q} P_{m_i}$ and $I \cap \left(P_{m_\alpha} \backslash \bigcup_{\alpha \neq \beta} P_{m_\beta} \right) \neq \emptyset$ for all $\alpha \neq \beta$, $\alpha, \beta = 1, ..., q$. with $q \in \mathbb{N}_{\geq 2}$.
Now choose, $a_i \in I \cap \left(P_{m_i} \backslash \bigcup_{i \neq \beta} P_{m_\beta} \right) \subseteq \left(P_{m_i} \backslash \bigcup_{i \neq \beta} P_{m_\beta} \right)$ for $i = 1, ..., q$.
By previous parts, we have $a_1 + a_2 a_3 ... a_q \notin \bigcup_{i=1}^{q} P_{m_i}$.
Now suppose $a_1 + a_2 a_3 ... a_q \in P_j \cap I$ such that $j \neq m_1, ..., m_q$. Since $j \neq m_1, ..., m_q$, $I \cap (P_j \backslash \bigcup_{i=1}^{q} P_{m_i}) = \emptyset$. Hence $I \cap P_j \subseteq I \cap \bigcup_{i=1}^{q} P_{m_i}$.(Contradiction! Since $a_1 + a_2 a_3 ... a_q \notin \bigcup_{i=1}^{q} P_{m_i}$). Hence $a_1 + a_2 a_3 ... a_q \notin \bigcup_{i=1}^{n} P_i$.(Contradiction! Since $I \subseteq \bigcup_{i=1}^{n} P_i$.) $\square$

Question 6

(a) Since F is a field $F[x]$ is a Euclidean Domain with the Euclidean function being the degree of the polynomial. Suppose $f(x) = p(x)q(x)$, then $\deg(f(x)) = \deg(p(x)) + \deg(q(x))$. Since $\deg(f(x)) = 1$, $\deg(p(x)) + \deg(q(x)) = 1$. Therefore one of $p(x), q(x)$ is of degree 0. Hence is a element of F and is a unit in $F[x]$. Therefore $f(x)$ is irreducible.

(b) Claim: If $f(a) = 0$ for some $a \in F$ then f is reducible.
Proof:
Since $F[x]$ is a Euclidean Domain, there exists $p(x), r(x)$ such that $f(x) = p(x)(x - a) + r(x)$. Since $f(a) = 0$, we have $r(a) = 0$ and since $\deg(r) = 0$, $r(x) = 0$. Hence $f(x) = p(x)(x - a)$. Since $\deg(f) = 2$, $\deg(p) = 1$. Hence f is reducible. $\square$

Claim: If f is reducible then $f(a) = 0$ for some $a \in F$. Proof:
Suppose f is reducible. Then $f(x) = p(x)q(x)$ such that $\deg(p) = \deg(q) = 1$. Hence $p(x) = (ax+b)$ for some $a, b \in F$. It is then clear that $f\left(\frac{-b}{a}\right) = 0$ and $\frac{-b}{a} \in F$ since F is a field.

(c) Since $(2)^3 - 2(2)^2 + 2 + 5 = 0 \bmod 7$. $x^3 - 2x^2 + x + 5 = (x - 2)(x^2 + ax + 1)$ for some $a \in F$. By comparing coefficients of x, we have $a = 0$. Since the order of $\mathbb{Z}_7*$ is 6 and the order of any x that satisfy $x^2 + 1 = 0$ is 4. But since $4 \nmid 6$, $x^2 + 1 = 0$ has no solution. Also 0 does not satisfy $x^2 + 1 = 0$. Hence $x^2 + 1$ is irreducible in $\mathbb{Z}_7[x]$.

Question 7

(a) For $n_1, n_2 \in N$, $n_1 = \sum_{i=1}^{k} r_i m_i$, $n_2 = \sum_{i=1}^{k} r_i' m_i$ such that $r_i, r_i' \in I$ and $\alpha \in R$.
Closed under addition

$$\begin{aligned} n_1 + n_2 &= \sum_{i=1}^{k} r_i m_i + \sum_{i=1}^{k} r_i' m_i \\ &= \sum_{i=1}^{k} (r_i + r_i') m_i \end{aligned}$$

. Since I is an ideal, $r_i + r_i' \in I$. Hence $n_1 + n_2 \in N$.
Closed under scalar multiplication

$$\begin{aligned} \alpha n_1 &= \alpha \sum_{i=1}^{k} r_i m_i \\ &= \sum_{i=1}^{k} (\alpha r_i) m_i \end{aligned}$$

. Since I is an ideal, $\alpha r_i \in I$. Hence $\alpha n_1 \in N$.
Therefore N is a submodule of M.

(b) Claim: $\{m_i + N \mid i = 1...k\}$ is a generating set for M/N
Proof:
For any $m + N \in M/N$, $m = \sum_{i=1}^{k} k_i m_i$ for $k_i \in R$ since $\{m_i \mid i = 1,..,k\}$ is a basis for M. Hence $m + M = \sum_{i=1}^{k} (k_i + I)(m_i + N)$. Therefore $\{m_i + N \mid i = 1...k\}$ is a generating set for M/N. $\square$

Claim: $\{m_i + N \mid i = 1...k\}$ is free.
Proof:
Let $(r_i + I) \in R/I$ for $i = 1, ..., k$.
Suppose we have $(r_1 + I)(m_1 + N) + (r_2 + I)(m_2 + N) + ... + (r_k + I)(m_k + N) = N$. Then we have

$$\begin{aligned} (r_1 m_1 + N) + (r_2 m_2 + N) + ... + (r_k m_k + N) &= N \\ (r_1 m_1 + r_2 m_2 + ... + r_k m_k) + N = N \end{aligned}$$

. Hence we have $r_1 m_1 + r_2 m_2 + ... + r_k m_k \in N$. Hence $r_i \in I$ for all $i = 1, ..., k$. $\square$

(c) Let $\{m_1, ..., m_k\}$ and $\{m_1', ..., m_l'\}$ be bases for M.

Claim: $\{\sum_{i=1}^{k} r_i m_i \mid r_i \in I \text{ for } i = 1 = 1, ..., k\} = \{\sum_{i=1}^{l} r_i m_i' \mid r_i \in I \text{ for } i = 1, ..., l\}$.
Proof:
Since $\{m_1, ..., m_k\}$ is a basis for M, we can express each m_i' for $i = 1, ..., l$ as a linear combination of $\{m_1, ..., m_k\}$. Since I is and ideal we would have $\{\sum_{i=1}^{k} r_i m_i \mid r_i \in I \text{ for } i = 1 = 1, ..., k\} \supseteq \{\sum_{i=1}^{l} r_i m_i' \mid r_i \in I \text{ for } i = 1, ..., l\}$. Similarly, since $\{m_1', ..., m_l'\}$ is a basis for M and I is an ideal,$\{\sum_{i=1}^{k} r_i m_i \mid r_i \in I \text{ for } i = 1 = 1, ..., k\} \subseteq \{\sum_{i=1}^{l} r_i m_i' \mid r_i \in I \text{ for } i = 1, ..., l\}$.
Hence we have$\{\sum_{i=1}^{k} r_i m_i \mid r_i \in I \text{ for } i = 1 = 1, ..., k\} = \{\sum_{i=1}^{l} r_i m_i' \mid r_i \in I \text{ for } i = 1, ..., l\}$.

Let $N = \{\sum_{i=1}^{k} r_i m_i \mid r_i \in I \text{ for } i = 1 = 1, ..., k\} = \{\sum_{i=1}^{l} r_i m_i' \mid r_i \in I \text{ for } i = 1, ..., l\}$.
By the previous part, we know that $\{m_1 + N, ..., m_k + N\}$ and $\{m_1' + N, ..., m_l' + N\}$ are bases for R/I module M/N. Since all finite bases for R/I modules have equal cardinality. We have $k = l$.
Hence any two finite bases for the R module M has equal cardinality.

Question 8

(a) For $n_1, n_2 \in \bigcup_{i=1}^{\infty}$, $n_1 \in M_i$, $n_2 \in M_j$ for some $i, j \in \mathbb{N}$. Therefore, $n_1, n_2 \in M_{\max(i,j)}$. Hence, $n_1 + n_2 \in M_{\max(i,j)} \subseteq \bigcup_{i=1}^{\infty}$. Therefore $\bigcup_{i=1}^{\infty}$ is closed under addition.
Since $n_1 \in M_i$ and $\alpha \in R$ and M_i is a module, $\alpha n_1 \in M_i \subseteq \bigcup_{i=1}^{\infty}$. Hence $\bigcup_{i=1}^{\infty}$ is closed under scalar multiplication.
Therefore $\bigcup_{i=1}^{\infty}$ is a submodule of M.

(b) Claim: There exists $g_1, ..., g_r, ...$ such that if $M_i = Rg_1 + Rg_2 + ... + Rg_i$ for $i \in \mathbb{N}$ then $M_1 \subsetneq M_2 \subsetneq ... \subsetneq M_r \subseteq ....$

Pick $g_1 \in M$. Now suppose $g_1, ..., g_n \in M$ have been chosen such that $M_i = Rg_1 + Rg_2 + ... + Rg_i$ for $i = 1, ..., n$ and $M_1 \subsetneq M_2 \subsetneq ... \subsetneq M_n$. Since M is not finitely generated, $M \backslash M_n = M \backslash Rg_1 + Rg_2 + ... + Rg_n \neq \emptyset$. Hence we choose $g_{n+1} \in M \backslash M_n$. Since $g_{n+1} \notin M_n$, $M_{n+1} = Rg_1 + Rg_2 + ... + Rg_{n+1} \supsetneq M_n$. By induction, we are able to choose $g_1, g_2, ..., g_r, ...$ such that if $M_i = Rg_1 + Rg_2 + ... + Rg_i$ for $i \in \mathbb{N}$ then $M_1 \subsetneq M_2 \subsetneq ... \subsetneq M_r \subseteq ....$ $\square$

(c) *Note: This question should read "M is Noetherian if and only if every submodule of M is finitely generated."*

Claim: M is Noetherian if every submodule of M is finitely generated.
Proof:
Suppose not. Then there exists a ascending chain of submodule $M_1 \subseteq M_2 \subseteq M_3 \subseteq ... \subseteq M_n \subseteq ...$ such that for any $k \in N$ there exists $j > k$ such that $N_j \supsetneq N_k$.
Consider the submodule $\bigcup_{i=1}^{\infty} N_i$, since $\bigcup_{i=1}^{\infty} N_i$ is finitely generated. There exists $\{n_1, ..., n_k\}$ that generates $\bigcup_{i=1}^{\infty} N_i$. Let N_p be the submodule that contains all $n_1, ..., n_k$. Hence $N_p = \bigcup_{i=1}^{\infty} N_i$. Also for all $j \geq p$, $N_j = \bigcup_{i=1}^{\infty} N_i = N_p$(Contradiction!). $\square$

Claim: If M is Noetherian then every submodule of M is finitely generated.
Proof:
Suppose not. Then there exists a submodule N of M such that N is not finitely generated. By the previous, we are able to generate a ascending sequence $\{P_i \mid i \in \mathbb{N}\}$ of submodules such that $P_i \subsetneq P_{i+1}$(Contradiction! Since M is Noetherian). $\square$

Hence M is Noetherian if and only if every submodule of M is finitely generated.