ALGEBRA II SOLUTIONS

Medium Test, 2011.04.18

1.

Let $M \subset R$ be the maximal ideal and assume M is not prime. That is there are $a,\ b \in R - M$ but $ab \in M$. Since R with unit, $R = R^2$. Since M is a maximal ideal and $a,\ b \in R - M$, $M + (a) = R$ and $M + (b) = R$. So

$$R = R^2 = (M + (a))(M + (b)) = M^2 + (a)M + (b)M + (a)(b) \subset M + (a)(b).$$

Since

$$(a)(b) = \{xayb|x, y \in R\} = \{xyab|x, y \in R\} \subset \{zab|z \in R\} = (ab) \subset M,$$

we have $R \subset M$, but it's impossible. Hence M is a prime ideal.

2.

Assume there is an ideal such that $M \subset N \subset R$ and $M \neq N$. That is there is an element in $N - M$ say $x + yi$. Note that $x + yi = y(2 + i) + (x - 2y)$ and we claim $(x - 2y, 5) = 1$. If the claim is false, that is $x - 2y = 5k$ for some integer k, then $x - 2y = 5k = k(2 - i)(2 + i)$. So

$$x + yi = y(2 + i) + (x - 2y) = y(2 + i) + k(2 - i)(2 + i) = [y + k(2 - i)](2 + i),$$

which is in M. It's impossible. Hence the claim is true.

Since $(x - 2y, 5) = 1$, there exist integers $a,\ b$ such that $(x - 2y)a + 5b = 1$. That is

$$1 = (x - 2y)a + 5b = (x + yi)a - ya(2 + i) + (2 - i)b(2 + i) \in N.$$

So $N = R$ and hence M is a maximal ideal.

3.

Let R be a Euclidean ring. Then there is a function $d : R - \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ such that (1) for all $a,\ b \in R - \{0\}$, $d(a) \leq d(ab)$, and (2) for all $a,\ b \in R - \{0\}$, there are $q,\ r \in R$ such that $b = qa + r$ with $r = 0$ or $d(r) < d(a)$.

Let $I \subset R$ be an ideal. Since $d(I - \{0\}) \subset \mathbb{N} \cup \{0\}$ and $\mathbb{N} \cup \{0\}$ has the well-ordering property, there exist $a \in I$ such that $d(a) = min\{d(x)|x \in I\}$.

Claim: $I = \{xa|x \in R\}$.

It's clear that $I \supset \{a|x \in R\}$, because $a \in I$. Now for all $b \in I - \{0\}$, there are $q,\ r \in R$ such that $b = qa + r$ with $r = 0$ or $d(r) < d(a)$.

Since $r = b - qa \in I$ and $d(a) = min\{d(x)|x \in I\}$, $r = 0$. That is $b = qa \in \{a|x \in R\}$. Therefore $I = \{xa|x \in R\}$ is principal.

4.

If $f(x) = 0 \in F[x]$, then $\forall g(x) \in F[x]$, $f(x)g(x) = 0 \neq 1$. So 0 is not invertible.

Let $f(x) \neq 0 \in F[x]$ which is invertible, and say $f(x)g(x) = 1$ for some $g(x) \in F[x]$. By Lemma 4.5.2,

$$deg(f(x)g(x)) = deg(f(x)) + deg(g(x)) \geqslant 0.$$

Since $deg(f(x)g(x)) = deg(1) = 0$, and $deg(f(x)) \geqslant 0$, and $deg(g(x)) \geqslant 0$, $deg(f(x)) = deg(g(x)) = 0$. So $f(x) = a$ is a nonzero constant in F.

5.

(1) Since $3|3,\ 3|(-6),\ 3^2 \nmid (-6)$, by Eisenstein criterion, $x^4 + 3x^2 + 3x - 6$ is irreducible.

(2) $x^5 - 5x^3 - 2x^2 + 10 = (x^3 - 2)(x^2 - 5)$ is not irreducible.

(3) Let $f(x) = x^3 + 3x + 2$ and $g(x) = f(x+1) = x^3 + 3x^2 + 6x + 6$. Since $3|3,\ 3|6,\ 3^2 \nmid 6$, by Eisenstein criterion, $g(x)$ is irreducible. Assume $f(x)$ is not irreducible. Then there are $f_1(x)$ and $f_2(x)$ in $\mathbb{Q}[x]$ such that $f(x) = f_1(x)f_2(x)$. So

$$g(x) = f(x+1) = f_1(x+1)f_2(x+1)$$

is not irreducible, but it's impossible. Hence $x^3 + 3x + 2$ is irreducible.

6.

Let $\varphi \in Aut(\mathbb{Q}[x])$, then we have $\varphi(0) = 0$. Suppose $\varphi(1) = 0$, then for all $f(x) \in \mathbb{Q}[x]$, $\varphi(f(x)) = \varphi(1 \cdot f(x)) = \varphi(1)\varphi(f(x)) = 0$, it's impossible. So $\varphi(1) \neq 0$. Since $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ and $\mathbb{Q}[x]$ is an integral domain (because $\mathbb{Q}$ is a field), we have $\varphi(1) = 1$.

(1) For all $n \in \mathbb{N}$,

$$\begin{aligned} \varphi(n) &= \varphi(1+1+...+1) \ (n\ times) \\ &= n\varphi(1) \\ &= n. \end{aligned}$$

(2) For all $m,\ n \in \mathbb{N}$,

$$\begin{aligned} n &= \varphi(n) \\ &= \varphi(\frac{n}{m} \cdot m) \\ &= \varphi(\frac{n}{m})\varphi(m) \\ &= m\varphi(\frac{n}{m}), \end{aligned}$$

that is $\varphi(\frac{n}{m}) = \frac{n}{m}$. Hence for all $a \in \mathbb{Q}^+ = \{x \in \mathbb{Q} | x > 0\}$, $\varphi(a) = a$.

Note that $0 = \varphi(0) = \varphi(1-1) = \varphi(1) + \varphi(-1)$. So $\varphi(-1) = -1$.

(3)For all $a \in \mathbb{Q}^- = \{x \in \mathbb{Q} | x < 0\}$,

$$\begin{aligned} \varphi(a) &= \varphi((-1) \cdot (-a)) \\ &= \varphi((-1))\varphi(-a)) \\ &= a. \end{aligned}$$

By (1), (2) and (3), For all $a \in \mathbb{Q},\ \varphi(a) = a$.

7.

Define $\varphi : F \longrightarrow K$ by $\varphi(\frac{r}{s}) = rs^{-1}$, where $r,\ s \in D,\ s \neq 0.$ and let $r,\ s,\ r_1,\ s_1 \in D,\ s \neq 0,\ s_1 \neq 0.$

Claim: $F \cong \varphi(F)$

Check: φ is well-define

If $\frac{r}{s} = \frac{r_1}{s_1}$, then $rs_1 = r_1 s \in D$. That is $rs^{-1} = r_1 s_1^{-1} \in K$. Hence $\varphi(\frac{r}{s}) = \varphi(\frac{r_1}{s_1})$.

Check: φ is homomorphism

$$\begin{aligned}
\varphi(\frac{r}{s} + \frac{r_1}{s_1}) &= \varphi(\frac{rs_1 + r_1 s}{ss_1}) \\
&= (rs_1 + r_1 s)(ss_1)^{-1} \\
&= rs^{-1} + r_1 s_1^{-1} \\
&= \varphi\frac{r}{s}) + \varphi(\frac{r_1}{s_1}).\varphi(\frac{r}{s} \cdot \frac{r_1}{s_1}) \\
&= \varphi(\frac{rr_1}{ss_1}) \\
&= (rr_1)(ss_1)^{-1} \\
&= (rs^{-1})(r_1 s_1^{-1}) \\
&= \varphi(\frac{r}{s})\varphi(\frac{r_1}{s_1}).
\end{aligned}$$

Check: φ is one to one

Let $\frac{r}{s} \in \ker(\varphi)$, that is $\varphi(\frac{r}{s}) = 0$. So we have $rs^{-1} = 0$, and thus $r = 0$ in D. Hence $\frac{r}{s} = 0$ in F.

So we have $F \cong \varphi(F)$.

Check: $D \subset \varphi(F)$

For all $a \in D$ with $a \neq 0$, $\varphi(\frac{aa}{a}) = aaa^{-1} = a$.

Let $F' = \varphi(F)$, then $D \subset F' \subset K$.

8.

Consider $\begin{pmatrix} i_1 & i_2 & ... & i_n \\ 1 & 2 & ... & n \end{pmatrix}$, then

$$\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}\begin{pmatrix} i_1 & i_2 & ... & i_n \\ 1 & 2 & ... & n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & ... & i_n \\ i_1 & i_2 & ... & i_n \end{pmatrix} = id$$

and

$$\begin{pmatrix} i_1 & i_2 & ... & i_n \\ 1 & 2 & ... & n \end{pmatrix}\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix} = id.$$

So the inverse of $\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$ is $\begin{pmatrix} i_1 & i_2 & ... & i_n \\ 1 & 2 & ... & n \end{pmatrix}$.

9.

Case1: Suppose $\tau(i) = j$, $i \neq j$. Since σ, τ are disjoint, $\sigma(j) = j$, $\sigma(i) = i$. Therefore $\sigma\tau(i) = \sigma(j) = j$, and $\tau\sigma(i) = \tau(i) = j$.

Case2: Suppose $\sigma(i) = j$, $i \neq j$. Since σ, τ are disjoint, $\tau(j) = j$, $\tau(i) = i$. Therefore $\sigma\tau(i) = \sigma(i) = j$, and $\tau\sigma(i) = \tau(j) = j$.

Case3: Suppose $\sigma(i) = i$, $\tau(i) = i$, then $\sigma\tau(i) = \sigma(i) = i$, and $\tau\sigma(i) = \tau(i) = i$.

So $\sigma\tau = \tau\sigma$, and hence $\sigma = \tau\sigma\tau^{-1}$.

10.

Given $\tau = \begin{pmatrix} i_1 & i_2 & ... & i_k \end{pmatrix}$, and any permutation σ.

Claim: $\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & ... & \sigma(i_k) \end{pmatrix}$.

For all $j = 1, 2, ..., k-1$, $\sigma\tau\sigma^{-1}(\sigma(i_j)) = \sigma\tau(i_j) = \sigma(i_{j+1})$, and $\sigma\tau\sigma^{-1}(\sigma(i_k)) = \sigma\tau(i_k) = \sigma(i_1)$.

For all $s \notin \{\sigma(i_1),\ \sigma(i_2), ...,\ \sigma(i_k)\}$, $\sigma^{-1}(s) \notin \{i_1,\ i_2, ...,\ i_k\}$, that is $\tau\sigma^{-1}(s) = \sigma^{-1}(s)$. So $\sigma\tau\sigma^{-1}(s) = \sigma\sigma^{-1}(s) = s$.

Hence $\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & ... & \sigma(i_k) \end{pmatrix}$ is a k-cycle.