November 21, 2006

Algebra II Final 2006

In the following, when R is a commutative ring with 1, $\langle a \rangle = \{r \cdot a \mid r \in R\}$, which is denoted by (a) in the textbook.

1. Let R be an integral domain. (40pts)

   (a) Let $a, b \in R$. Show that the following are equivalent.

      (i) $a \mid b$ and $b \mid a$.

      (ii) $\langle a \rangle = \langle b \rangle$.

      (iii) $a \approx b$, i.e., there exists $u \in U(R)$ such that $b = ua$, where u is a unit of R.

   (b) Show that the polynomial ring $R[t]$ is an integral domain.

   (c) Show that $U(R[t]) = U(R)$.

   (d) Let p be a nonzero element in R such that $p \notin U(R)$. Suppose $\langle p \rangle$ is a prime ideal. Show that p is an irreducible element.

2. Let $\boldsymbol{Q}[t]$, the polynomial ring over the rational number field $\boldsymbol{Q}$. Let $f(t) = t^5 + 6t - 12$. Let α be the unique real root of $f(t) = 0$, and $\boldsymbol{Q}[\alpha] = \{g(\alpha) \mid g(t) \in \boldsymbol{Q}[t]\}$. (30pts)

   (a) Show that $f(t)$ is an irreducible element in an integral domain $\boldsymbol{Q}[t]$.

   (b) Let $\theta : \boldsymbol{Q}[t] \to \boldsymbol{Q}[\alpha] \subset \boldsymbol{R}$ $(g(t) \mapsto g(\alpha))$. Show that $\mathrm{Ker}(\theta) = \langle f(t) \rangle$.

   (c) Show that $\boldsymbol{Q}[\alpha]$ is a field.

3. Let $R = \{a + b\sqrt{-3} \mid a, b \in \boldsymbol{Z}\}$. (20pts)

   (a) Show that 2, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are irreducible elements in R.

   (b) Show that R is not a UFD.

4. Using a theorem that states that if R is a UFD, then the polynomial ring $R[t]$ in t over R is a UFD, show that the polynomial ring $R[t_1, t_2, \ldots, t_n]$ in t_1, $t_2, \ldots, t_n$ over R is a UFD. (10pts)

Solutions to Algebra II Final 2006

1. Let R be an integral domain. (40pts)

   (a) Let $a, b \in R$. Show that the following are equivalent.

   (i) $a \mid b$ and $b \mid a$.

   (ii) $\langle a \rangle = \langle b \rangle$.

   (iii) $a \approx b$, i.e., there exists $u \in U(R)$ such that $b = ua$, where u is a unit of R.

   Solution. (i)→(ii): Since $a \mid b$ and $b \mid a$, there exist c, $d \in R$ such that $b = ac$ and $a = bd$. Hence $b \in \langle a \rangle$ and $a \in \langle b \rangle$. Therefore $\langle b \rangle \subseteq \langle a \rangle$ and $\langle a \rangle \subseteq \langle b \rangle$. Thus $\langle a \rangle = \langle b \rangle$.

   (ii)→(iii): Since $\langle a \rangle = \langle b \rangle$, if $a = 0$, then $b = 0$ and we can take 1 for u. Assume that $a \neq 0$. Since a, $b \in \langle a \rangle = \langle b \rangle$, there exist u, $v \in R$ such that $a = vb$, $b = ua$. Hence $a = vb = vua$ and $a(1 - vu) = 0$. Since R is an integral domain and $a \neq 0$, $1 = vu = uv$ and $u \in U(R)$. Thus $b = ua$ with $u \in U(R)$.

   (iii)→(i): Let $b = ua$ with $u \in U(R)$. Then $a \mid b$. Since $a = u^{-1}b$, $b \mid a$. ∎

   (b) Show that the polynomial ring $R[t]$ is an integral domain.

   Solution. Since R is an integral domain, $\deg(f \cdot g) = \deg(f) + \deg(g)$ holds for $f, g \in R[t]$. If $f \cdot g = 0$, then $-\infty = \deg(f \cdot g) = \deg(f) + \deg(g)$. Hence either $\deg(f) = -\infty$ or $\deg(g) = -\infty$. Therefore either $f = 0$ or $g = 0$ and $R[t]$ is an integral domain. ∎

   (c) Show that $U(R[t]) = U(R)$.

   Solution. It is clear that $U(R[t]) \supseteq U(R)$. Suppose $1 = f \cdot g$. Then $0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g)$. Hence $\deg(f) = \deg(g) = 0$. Therefore $f, g \in R$. Since $f \cdot g = 1$, $f \in U(R)$. ∎

   (d) Let p be a nonzero element in R such that $p \notin U(R)$. Suppose $\langle p \rangle$ is a prime ideal. Show that p is an irreducible element.

   Solution. Suppose $p = a \cdot b$. Then $\langle p \rangle \subseteq \langle a \rangle$, and $\langle p \rangle \subseteq \langle b \rangle$. Since $\langle p \rangle$ is a prime ideal, either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. Thus either $\langle a \rangle \subseteq \langle p \rangle$ or $\langle b \rangle \subseteq \langle p \rangle$. Therefore, either $\langle a \rangle = \langle p \rangle$ or $\langle b \rangle = \langle p \rangle$. Now by 1, either $b \in U(R)$ or $a \in U(R)$. ∎

2. Let $\boldsymbol{Q}[t]$, the polynomial ring over the rational number field $\boldsymbol{Q}$. Let $f(t) = t^5 + 6t - 12$. Let α be the unique real root of $f(t) = 0$, and $\boldsymbol{Q}[\alpha] = \{g(\alpha) \mid g(t) \in \boldsymbol{Q}[t]\}$. (30pts)

   (a) Show that $f(t)$ is an irreducible element in an integral domain $\boldsymbol{Q}[t]$.

   Solution. By Eisenstein's criterion taking $p = 3$, $f(t)$ is irreducible over $\boldsymbol{Z}$. By Gauss' lemma, it is irreducible over $\boldsymbol{Q}$. Since $\boldsymbol{Q}$ is a field, $f(t)$ is an irreducible element. ■

   (b) Let $\theta : \boldsymbol{Q}[t] \to \boldsymbol{Q}[\alpha] \subset \boldsymbol{R}$ $(g(t) \mapsto g(\alpha))$. Show that $\mathrm{Ker}(\theta) = \langle f(t) \rangle$.

   Solution. It is clear that θ is a surjective ring homomorphism, and that $\mathrm{Ker}(\theta) \supseteq \langle f(t) \rangle$. Since $\boldsymbol{Q}[t]$ is an Euclidean domain, $\boldsymbol{Q}[t]$ is a PID. Since $\mathrm{Ker}(\theta)$ is an ideal, there exists $p(t) \in R[t]$ such that $\mathrm{Ker}(\theta) = \langle p(t) \rangle \ni f(t)$. Since $f(t)$ is irreducible, $\mathrm{Ker}(\theta) = \langle p(t) \rangle = \langle f(t) \rangle$. ■

   (c) Show that $\boldsymbol{Q}[\alpha]$ is a field.

   Solution. By Isomorphism Theorm, $\boldsymbol{Q}[t]/\mathrm{Ker}(\theta) \simeq \boldsymbol{Q}[\alpha]$. Since $f(t)$ is an irreducible element in a PID $\boldsymbol{Q}[t]$, it generates a maximal ideal. Since $\mathrm{Ker}(\theta) = \langle f(t) \rangle$, $\boldsymbol{Q}[t]/\mathrm{Ker}(\theta)$ is a field, and so is $\boldsymbol{Q}[\alpha]$. ■

3. Let $R = \{a + b\sqrt{-3} \mid a, b \in \boldsymbol{Z}\}$. (20pts)

   (a) Show that 2, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are irreducible elements in R.

   Solution. Let $N(a + b\sqrt{-3}) = a^2 + 3b^2$. Then $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$. Hence if $\alpha \cdot \beta = 1$, then $1 = N(1) = N(\alpha)N(\beta)$ and $N(\alpha) = N(\beta) = 1$. Therefore, $U(R) = \{\pm 1\}$. Now $4 = N(2) = N(1 \pm \sqrt{-3})$. By definition there is no element $\alpha = a + b\sqrt{-3}$ such that $N(\alpha) = a^2 + 3b^2 = 2$, 2, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are irreducible elements in R. ■

   (b) Show that R is not a UFD.

   Solution. Since $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ gives two distinct representations of 4 as a product of irreducible elements which are not associate each other. Hence R is not a UFD. ■

4. Using a theorem that states that if R is a UFD, then the polynomial ring $R[t]$ in t over R is a UFD, show that the polynomial ring $R[t_1, t_2, \ldots, t_n]$ in $t_1, t_2, \ldots, t_n$ over R is a UFD. (10pts)

   Solution. We prove by induction on n. The theorem states the case when $n = 1$. By the induction hypothesis assume that $R[t_1, t_2, \ldots, t_{k-1}]$ is a UFD. Since

$$R[t_1, t_2, \ldots, t_k] = R[t_1, t_2, \ldots, t_{k-1}][t_k],$$

   $R[t_1, t_2, \ldots, t_k]$ can be regarded as a polynomial ring in t_k over a UFD $R[t_1, t_2, \ldots, t_{k-1}]$. Hence $R[t_1, t_2, \ldots, t_k]$ is a UFD. ■