November 17, 2005

Algebra II Final 2005

1. Let R be an integral domain and $a, b \in R$. Show that the following are equivalent.

   (a) $(a) \subseteq (b)$ and $(b) \subseteq (a)$.

   (b) There exists $u \in U(R)$ such that $b = ua$.

2. Find all units and zero divisors of $\boldsymbol{Z}_{18}$.

3. Let a, b be elements in an integral domain R. A *greatest common divisor* of a and b is a ring element d such that (i) $d \mid a$ and $d \mid b$; (ii) if $c \mid a$ and $c \mid b$ for some $c \in R$, then $c \mid d$.

   Show the following.

   (a) Let a and b be elements of a principal ideal domain R. Then a and b have a greatest common divisor d which has the form $d = ax + by$ with $x, y \in R$.

   (b) If R is a principal ideal domain and $p \mid bc$ where $p, b, c \in R$ and p is irreducible, then $p \mid b$ or $p \mid c$.

4. Let $\boldsymbol{Z}[t]$ be a polynomial ring in t over the ring of rational integers $\boldsymbol{Z}$. Let

$$\phi : \boldsymbol{Z}[t] \longrightarrow \boldsymbol{C} \ (f(t) \mapsto f(\sqrt{-1})).$$

   (You may assume that ϕ is a ring homomorphism.)

   (a) Show that $\boldsymbol{Z}[t]$ is an integral domain.

   (b) Let $R = \mathrm{Im}(\phi)$. Show that $R = \{a + b\sqrt{-1} \mid a, b \in \boldsymbol{Z}\}$, and R is an integral domain.

   (c) Show that $I = \mathrm{Ker}\phi$ is an ideal of $\boldsymbol{Z}[t]$. Show also that I is a prime ideal but not a maximal ideal.

   (d) Determine $U(R)$.

   (e) Show that 3 is a primitive element of R, but 2 is not.

   (f) Determine whether (5), the ideal generated by 5, is a prime ideal in R.

November 17, 2005

Solutions to Algebra II Final 2005

1. Let R be an integral domain and $a, b \in R$. Show that the following are equivalent.

   (a) $(a) \subseteq (b)$ and $(b) \subseteq (a)$.

   (b) There exists $u \in U(R)$ such that $b = ua$.

   Solution. (a)→(b): Since $(a) = (b)$, if $a = 0$, then $b = 0$ and we can take 1 for u. Assume that $a \neq 0$. Since a, $b \in (a) = (b)$, 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 $u \in U(R)$.

   (b)→(a): Let $b = ua$ with $u \in U(R)$. Then $b \in (a)$. Since $a = u^{-1}b$, we have $a \in (b)$ as well. Hence $(a) \subseteq (b)$ and $(b) \subseteq (a)$.

2. Find all units and zero divisors of $\boldsymbol{Z}_{18}$.

   Solution.

   units: $[1], [5], [7], [11], [13], [17]$.

   zero divisors: $[2], [3], [4], [6], [8], [9], [10], [12], [14], [15], [16]$.

3. Let a, b be elements in an integral domain R. A *greatest common divisor* of a and b is a ring element d such that (i) $d \mid a$ and $d \mid b$; (ii) if $c \mid a$ and $c \mid b$ for some $c \in R$, then $c \mid d$.

   Show the following.

   (a) Let a and b be elements of a principal ideal domain R. Then a and b have a greatest common divisor d which has the form $d = ax + by$ with $x, y \in R$.

   Solution. Recall that since R is an integral domain the following hold for a, $b \in R$:

   $$a \mid b \Leftrightarrow (b) \subseteq (a).$$

   Since $I = \{ax + by \mid x, y \in R\} = (a) + (b)$ is an ideal of an integral domain R, there exists $d \in R$ such that $I = (d)$. Since $d \in I$, there exist x, $y \in R$ such that $d = ax + by$. Since $(a) \subseteq (d)$ and $(b) \subseteq (d)$, $d \mid a$ and $d \mid b$.

   Suppose $c \mid a$ and $c \mid b$, then $(a) \subseteq (c)$ and $(b) \subseteq (c)$. Hence

   $$(d) = I = (a) + (b) \subseteq (c).$$

   Thus $c \mid d$. Therefore d is a greatest common divisor of a and b.

   (b) If R is a principal ideal domain and $p \mid bc$ where $p, b, c \in R$ and p is irreducible, then $p \mid b$ or $p \mid c$.

   Let $I = \{px + by \mid x, y \in R\}$. Since R is a principal ideal domain, there exists $d \in R$ such that $I = (d)$ and d is a greatest common divisor of p and b. In particular, $d \mid p$ and there exists $e \in R$ such that $p = de$. Since p is irreducible, either $d \in U(R)$ or $e \in U(R)$. Hence either $I = R$ or $I = (p)$. Suppose $I = (p)$. Since $(b) \subseteq I = (p)$, $p \mid b$. Suppose $I = R$. Then there exist x, $y \in R$ such that $1 = px + by$. Now $c = pcx + bcy$. Since $p \mid bc$ by assumption, and $p \mid pcx$, we have $p \mid c$. Thus $p \mid b$ or $p \mid c$.

4. Let $\boldsymbol{Z}[t]$ be a polynomial ring in t over the ring of rational integers $\boldsymbol{Z}$. Let

$$\phi : \boldsymbol{Z}[t] \longrightarrow \boldsymbol{C} \ (f(t) \mapsto f(\sqrt{-1})).$$

(You may assume that ϕ is a ring homomorphism.)

(a) Show that $\boldsymbol{Z}[t]$ is an integral domain.

Solution. Since $\boldsymbol{Z}$ is an integral domain and every polynomial ring over an integral domain is an integral domain, $\boldsymbol{Z}[t]$ is an integral domain.

(Let $0 \neq f = f_0 + f_1 t + \cdots + f_m t^m$ and $0 \neq g = g_0 + g_1 t + \cdots + g_n t^n$ with $f_m \neq 0$ and $g_n \neq 0$. Then $f \cdot g = f_0 g_0 + (f_0 g_1 + g_0 f_1)t + \cdots + f_m g_n t^{m+n}$. Since $\boldsymbol{Z}$ is an integral domain, $f_m g_n \neq 0$. Hence $f \cdot g \neq 0$. Thus $\boldsymbol{Z}[t]$ is an integral domain.)

(b) Let $R = \mathrm{Im}(\phi)$. Show that $R = \{a + b\sqrt{-1} \mid a, b \in \boldsymbol{Z}\}$, and R is an integral domain.

Solution. Since R is the image of a ring homomorphism, R is a subring of a field $\boldsymbol{C}$. Since a field does not have a zero divisor, R is an integral domain. Since $(\sqrt{-1})^m \in \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$, $\phi(f(t)) = f(\sqrt{-1}) \in \{a + b\sqrt{-1} \mid a, b \in \boldsymbol{Z}\}$. On the other hand, $\phi(a + bt) = a + b\sqrt{-1}$. Hence $R = \{a + b\sqrt{-1} \mid a, b \in \boldsymbol{Z}\}$.

(c) Show that $I = \mathrm{Ker}\phi$ is an ideal of $\boldsymbol{Z}[t]$. Show also that I is a prime ideal but not a maximal ideal.

Solution. Since ϕ is a ring homomorphism, its kernel is an ideal. By the isomorphism theorem, $\boldsymbol{Z}[t]/I = \boldsymbol{Z}[t]/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi) = R$. R is an integral domain as was shown in the previous problem. But R is not a field as $2^{-1} \notin R$. Hence I is a prime ideal but not a maximal ideal. Note that if I is an ideal of a commutative ring R, then R/I is an integral domain if and only if I is a prime ideal. Moreovere, R/I is a field if and only if I is a maximal ideal.

(d) Determine $U(R)$.

Solution. Let $N(a + b\sqrt{-1}) = (a + b\sqrt{-1})\overline{(a + b\sqrt{-1})} = a^2 + b^2$. Then for all $\alpha, \beta \in R$, $N(\alpha\beta) = N(\alpha)N(\beta)$. If $\alpha = a + b\sqrt{-1} \in R$ is a unit, then there exists $\beta \in R$ such that $\alpha\beta = 1$. Then $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$.Since $N(\alpha) = a^2 + b^2$ is a nonnegative integer and so is $N(\beta)$, $N(\alpha) = 1$. Thus $a^2 + b^2 = 1$ and $\alpha \in \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$. Since $\{1, -1, \sqrt{-1}, -\sqrt{-1}\} \subseteq U(R)$, we have $U(R) = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$. In particular, $\alpha \in U(R) \Leftrightarrow N(\alpha) = 1$.

(e) Show that 3 is a primitive (irreducible) element of R, but 2 is not.

Solution. Suppose $3 = \alpha\beta$ with $\alpha, \beta \in R \setminus U(R)$. Then $9 = N(3) = N(\alpha\beta) = N(\alpha)N(\beta)$. Since $N(\alpha) \neq 1$ and $N(\beta) \neq 1$, $N(\alpha) = N(\beta) = 3$. Let $\alpha = a + b\sqrt{-1}$. Then $3 = a^2 + b^2$. But this is impossible. Hence 3 is an irredubible element.

$2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$ and $N(1 + \sqrt{-1}) = N(1 - \sqrt{-1}) = 2 \neq 1$. Hence $1 + \sqrt{-1}, 1 - \sqrt{-1} \notin U(R)$. Hence 2 is not irreducible.

(f) Determine whether (5), the ideal generated by 5, is a prime ideal in R.

Solution. $(2 + \sqrt{-1})(2 - \sqrt{-1}) = 5 \in (5)$. Let $\alpha \in \{2 + \sqrt{-1}, 2 - \sqrt{-1}\}$ and $\alpha \in (5)$. Then $\alpha = 5\beta$ for some $\beta \in R$. Then $5 = N(\alpha) = N(5\beta) = N(5)N(\beta) = 25N(\beta)$. This is impossible. Hence (5) is not a prime ideal.