November 15, 2017

Algebra II Final 2017

1. Let $\boldsymbol{Z}$ be a ring of rational integers, $\boldsymbol{Z}[x]$ the polynomial ring in x over $\boldsymbol{Z}$ and $\boldsymbol{Z}[x, y]$ the polynomial ring in x and y over $\boldsymbol{Z}$. Show the following. (25pts)

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

   (b) $\boldsymbol{Z}[x, y]$ is an integral domain.

   (c) For the unit groups, $U(\boldsymbol{Z}[x, y]) = U(\boldsymbol{Z}[x]) = U(\boldsymbol{Z}) = \{1, -1\}$.

   (d) For $f(x, y), g(x, y) \in \boldsymbol{Z}[x, y]$, if $\langle f(x, y)\rangle = \langle g(x, y)\rangle$, then $f(x, y) = g(x, y)$ or $f(x, y) = -g(x, y)$.

   (e) For a nonzero polynomial $f(x, y) \in \boldsymbol{Z}[x, y]$, if $\langle f(x, y)\rangle$ is a prime ideal, then $f(x, y)$ is irreducible, i.e., $f(x, y) = g(x, y)h(x, y)$ for $g(x, y), h(x, y) \in \boldsymbol{Z}[x, y]$ implies $g(x, y) = \pm 1$ or $h(x, y) = \pm 1$.

2. Let $\boldsymbol{Z}_3[x]$ be the polynomial ring over $\boldsymbol{Z}_3$, $p(x)$ a polynomial in $\boldsymbol{Z}_3[x]$ of degree $n > 0$ and $R = \boldsymbol{Z}[x]/\langle p(x)\rangle$. Show the following. (25pts)

   (a) $R = \{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle p(x)\rangle \mid c_0, c_1, \ldots, c_{n-1} \in \boldsymbol{Z}_3\}$.

   (b) There are exactly 3^n elements in R.

   (c) If R is an integral domain, then it is a field.

   (d) R is an integral domain if and only if $p(x)$ is irreducible over $\boldsymbol{Z}_3$.

   (e) If $p(x) = x^4 + x + 2$, then R is a field with 81 elements.

3. Let R and S be commutative rings with unity 1, and $\phi : R \to S$ a ring homomorphism such that $\phi(1) = 1$. Show the following. (25pts)

   (a) If B is an ideal of S, then $A = \phi^{-1}(B) = \{x \in R \mid \phi(x) \in B\}$ is an ideal of R.

   (b) If B is a prime ideal of S, then $A = \phi^{-1}(B)$ is a prime ideal of R.

   (c) Let $R = \boldsymbol{Z}[x, y]$, $S = \boldsymbol{Z}[x]$ and $\phi : R \to S$ $(f(x, y) \mapsto f(x, 0))$. Then $\mathrm{Ker}\phi$ is a prime ideal but not a maximal ideal.

   (d) $\langle y\rangle$ is a prime ideal but not maximal in $R = \boldsymbol{Z}[x, y]$.

   (e) $\boldsymbol{Z}[x, y]$ is not a principal ideal domain.

4. Let $R = \{a + b\sqrt{-3} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$ and $\gamma = 1 + \sqrt{-3} \in R$, where $\boldsymbol{C}$ is the complex number field. Show the following. (25pts)

   (a) R is an integral domain.

   (b) $U(R) = \{1, -1\}$.

   (c) γ is an irreducible element.

   (d) $\langle\gamma\rangle$ is not a prime ideal.

   (e) R is not a unique factorization domain.

November 15, 2017

Solutions to Algebra II Final 2017

1. Let $\boldsymbol{Z}$ be a ring of rational integers, $\boldsymbol{Z}[x]$ the polynomial ring in x over $\boldsymbol{Z}$ and $\boldsymbol{Z}[x, y]$ the polynomial ring in x and y over $\boldsymbol{Z}$. Show the following. (25pts)

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

   Claim. If R is an integral domain, then the polynomial ring $R[x]$ is an integral domain.

   Proof. For nonzero polynomials $f(x) = a_m x^m + \cdots + a_m$, $g(x) = b_n x^n + \cdots + b_0$ with $a_m \neq 0$ and $b_n \neq 0$, $f(x)g(x) = a_m b_n x^{m+n} +$ lower terms. Since R is an integral domain, $a_m b_n \neq 0$ and $f(x)g(x) \neq 0$. ■

   Solution. Since $\boldsymbol{Z}$ is an integral domain, by the claim above, $\boldsymbol{Z}[x]$ is an integral domain. ■

   (b) $\boldsymbol{Z}[x, y]$ is an integral domain.

   Solution. Since every polynomial $f(x, y) \in \boldsymbol{Z}[x, y]$ can be written as $f(x, y) = f_n(y)x^n + f_{n-1}(y)x^{-1} + \cdots + f_0(x)$, where $f_n(y), f_{n-2}(y), \ldots, f_0(y) \in \boldsymbol{Z}[y]$. Hence $\boldsymbol{Z}[x, y]$ is a polynomial ring in x over $\boldsymbol{Z}[y]$. Since $\boldsymbol{Z}[y]$ is an integral domain by (a) and by the claim above, $(\boldsymbol{Z}[y])[x] = \boldsymbol{Z}[x, y]$ is an integral domain. ■

   (c) For the unit groups, $U(\boldsymbol{Z}[x, y]) = U(\boldsymbol{Z}[x]) = U(\boldsymbol{Z}) = \{1, -1\}$.

   Claim. If R is an integral domain, then $U(R[x]) = U(R)$.

   Proof. $U(R[x]) \supset U(R)$ is clear. For nonzero polynomials $f(x) = a_m x^m + \cdots + a_m$, $g(x) = b_n x^n + \cdots + b_0$ with $a_m \neq 0$ and $b_n \neq 0$, suppose $1 = f(x)g(x) = a_m b_n x^{m+n} +$ lower terms. This is possible only if $m = n = 0$ and $a_m b_n = 1$. Hence $U(R[x]) \subset U(R)$. ■

   Solution. By the observation in the solution of (b) and the claim above,

   $$U(\boldsymbol{Z}[x, y]) = U((\boldsymbol{Z}[y])[x]) = U(\boldsymbol{Z}[y]) = U(\boldsymbol{Z}).$$

   Similarly, $U(\boldsymbol{Z}[x]) = U(\boldsymbol{Z})$. Since $ab = 1$ for $a, b \in \boldsymbol{Z}$ implies $a, b \in \{1, -1\}$, the assertion follows. ■

   (d) For $f(x, y), g(x, y) \in \boldsymbol{Z}[x, y]$, if $\langle f(x, y)\rangle = \langle g(x, y)\rangle$, then $f(x, y) = g(x, y)$ or $f(x, y) = -g(x, y)$.

   Solution. Suppose $\langle f(x, y)\rangle = \langle g(x, y)\rangle$. If $f(x, y) = 0$, then $g(x, y) = 0$. Hence $f(x, y) = g(x, y)$ in this case. Suppose that $f(x, y) \neq 0$. Since $f(x, y) \in \langle g(x, y)\rangle$, $f(x, y) = h(x, y)g(x, y)$ for some $h(x, y) \in \boldsymbol{Z}[x, y]$. Similarly, it follows from $g(x, y) \in \langle f(x, y)\rangle$ that there is $k(x, y) \in \boldsymbol{Z}[x, y]$ such that $g(x, y) = k(x, y)f(x, y)$. Hence $f(x, y)(1 - h(x, y)k(x, y)) = 0$. Since $f(x, y) \neq 0$ and $\boldsymbol{Z}[x, y]$ is an integral domain by (b), $h(x, y)k(x, y) = 1$ and $h(x, y) \in U(\boldsymbol{Z}[x, y]) = \{1, -1\}$ by (c). Since $f(x, y) = h(x, y)g(x, y)$, $f(x, y) = g(x, y)$ or $f(x, y) = -g(x, y)$. ■

   (e) For a nonzero polynomial $f(x, y) \in \boldsymbol{Z}[x, y]$, if $\langle f(x, y)\rangle$ is a prime ideal, then $f(x, y)$ is irreducible, i.e., $f(x, y) = g(x, y)h(x, y)$ for $g(x, y), h(x, y) \in \boldsymbol{Z}[x, y]$ implies $g(x, y) = \pm 1$ or $h(x, y) = \pm 1$.

Solution. Suppose $g(x,y)h(x,y) = f(x,y) \in \langle f(x,y)\rangle$ and $\langle f(x,y)\rangle$ is a prime ideal. Clearly, $f(x,y) \in \langle g(x,y)\rangle \cap \langle h(x,y)\rangle$. Hence $\langle f(x,y)\rangle \subset \langle g(x,y)\rangle \cap \langle h(x,y)\rangle$. Since $\langle f(x,y)\rangle$ is a prime ideal, $g(x,y) \in \langle f(x,y)\rangle$ or $h(x,y) \in \langle f(x,y)\rangle$. Hence $\langle g(x,y)\rangle \subset \langle f(x,y)\rangle$ or $\langle h(x,y)\rangle \subset \langle f(x,y)\rangle$. Therefore, $\langle g(x,y)\rangle = \langle f(x,y)\rangle$ or $\langle h(x,y)\rangle = \langle f(x,y)\rangle$. By (d), $f(x,y) = \pm g(x,y)$ or $f(x,y) = \pm h(x,y)$. Since $f(x,y) = g(x,y)h(x,y)$ and $f(x,y)$ is nonzero, $g(x,y) = \pm 1$ or $h(x,y) = \pm 1$. ■

2. Let $\boldsymbol{Z}_3[x]$ be the polynomial ring over $\boldsymbol{Z}_3$, $p(x)$ a polynomial in $\boldsymbol{Z}_3[x]$ of degree $n > 0$ and $R = \boldsymbol{Z}[x]/\langle p(x)\rangle$. Show the following. (25pts)

   (a) $R = \{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle p(x)\rangle \mid c_0, c_1, \ldots, c_{n-1} \in \boldsymbol{Z}_3\}$.
   Solution. Let $f(x) \in \boldsymbol{Z}_3[x]$. Since $\boldsymbol{Z}_3$ is a field, $\boldsymbol{Z}_3[x]$ is a Euclidian domain and there exist $q(x), r(x) \in \boldsymbol{Z}_3[x]$ such that $\deg r(x) < \deg p(x) = n$ such that $f(x) = q(x)p(x) + r(x)$. Since there exist $c_0, c_1, \ldots, c_{n-1} \in \boldsymbol{Z}_3$ such that $r(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$,

$$f(x) + \langle p(x)\rangle = r(x) + q(x)p(x) + \langle p(x)\rangle = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle p(x)\rangle.$$

   Thus $R = \{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle p(x)\rangle \mid c_0, c_1, \ldots, c_{n-1} \in \boldsymbol{Z}_3\}$. ■

   (b) There are exactly 3^n elements in R.
   Solution. Suppose $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle p(x)\rangle = c'_0 + c'_1 x + \cdots + c'_{n-1}x^{n-1} + \langle p(x)\rangle$. Then

$$(c_0 - c'_0) + (c_1 - c'_1)x + \cdots + (c_{n-1} - c'_{n-1})x^{n-1} \in \langle p(x)\rangle.$$

   Since $\deg p(x) = n$, this is possible only when $c_0 = c'_0$, $c_1 = c'_1$, $\ldots$, $c_{n-1} = c'_{n-1}$, and the expression $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + \langle p(x)\rangle$ is unique. Thus, there are 3^n choices of $c_0, c_1, \ldots, c_{n-1} \in \boldsymbol{Z}_3$ and there are exactly 3^n elements in R. ■

   (c) If R is an integral domain, then it is a field.
   Solution. R is a finite commutative ring with unity. Suppose R is an integral domain. If $\alpha \in R$ is a nonzero element, then an additive homomorphism

$$\lambda_\alpha : R \to R\ (\beta \mapsto \alpha\beta)$$

   is one-to-one as $\mathrm{Ker}\lambda_\alpha = \{0\}$. Note that $0 = \lambda_\alpha(\beta) = \alpha\beta$ implies that $\beta = 0$ as α is nonzero and R is an integral domain. Since R is finite, $|\lambda_\alpha(R)| = |R|$ implies that λ_α is onto and there exists $\beta \in R$ such that $\alpha\beta = 1$. Hence R is a field. ■

   (d) R is an integral domain if and only if $p(x)$ is irreducible over $\boldsymbol{Z}_3$.
   Solution. If $q(x)r(x) \in \langle p(x)\rangle$, then

$$(q(x) + \langle p(x)\rangle)(r(x) + \langle p(x)\rangle) = q(x)r(x) + \langle p(x)\rangle = \langle p(x)\rangle.$$

   Hence if R is an integral domain, $q(x) \in \langle p(x)\rangle$ or $r(x) \in \langle p(x)\rangle$. In particular, if $q(x)r(x) = p(x)$, then $p(x)$ divides either $q(x)$ or $r(x)$ and $p(x)$ is irreducible. Conversely, if $p(x)$ is irreducible, $p(x)$ divides $q(x)$ or $r(x)$ as $\boldsymbol{Z}_3[x]$ is a unique factorization domain. Therefore, $q(x) \in \langle p(x)\rangle$ or $r(x) \in \langle p(x)\rangle$ and $\langle p(x)\rangle$ is a prime ideal. ■

(e) If $p(x) = x^4 + x + 2$, then R is a field with 81 elements.

Solution. We claim that $p(x)$ is irreducible. Since $p(0) = p(2) = 2, p(1) = 1$ and $p(x)$ does not have a factor of degree one. Let $x^4 + x + 2 = (x^2 + ax + b)(x^2 + cx + d)$ be a product of irreducible polynomials of degree two. We may assume $b = 1$ and $d = 2$. Then $a = 0$ and $c \neq 0$ by irreducibility. This is impossible as $a + c$ is the coefficient of x^3 in $p(x)$.

3. Let R and S be commutative rings with unity 1, and $\phi : R \to S$ a ring homomorphism such that $\phi(1) = 1$. Show the following. (25pts)

(a) If B is an ideal of S, then $A = \phi^{-1}(B) = \{x \in R \mid \phi(x) \in B\}$ is an ideal of R.

Solution. Let $x, y \in A$ and $r \in R$. Then $\phi(x - y) = \phi(x) - \phi(y) \in B$ and $\phi(rx) = \phi(r)\phi(x) \in B$. Hence A is an ideal. ■

(b) If B is a prime ideal of S, then $A = \phi^{-1}(B)$ is a prime ideal of R.

Solution. By (a), A is an ideal. If $A = R$, $1 \in A = \phi^{-1}(B)$ and $\phi(1) = 1 \in B$. Thus $B = S$, which is not the case as a prime ideal is proper. Suppose $xy \in A$. Then $\phi(x)\phi(y) = \phi(xy) \in B$. Since B is a prime ideal, $\phi(x) \in B$ or $\phi(y) \in B$. Thus $x \in \phi^{-1}(B) = A$ or $y \in \phi^{-1}(B) = A$. Thus A is a prime ideal. ■

(c) Let $R = \boldsymbol{Z}[x, y]$, $S = \boldsymbol{Z}[x]$ and $\phi : R \to S(f(x, y) \mapsto f(x, 0))$. Then $\mathrm{Ker}\phi$ is a prime ideal but not a maximal ideal.

Solution. First note that ϕ is a ring homomorphism. Since $\boldsymbol{Z}[x]$ is an integral domain by 1(a), $\langle 0 \rangle$ is a prime ideal. Hence by (c), $\mathrm{Ker}\phi$ is a prime ideal. Since for $f(x) \in \boldsymbol{Z}[x]$, $\phi(f(x)) = f(x)$, ϕ is onto. By the isomorphism theorem, $\boldsymbol{Z}[x, y]/\mathrm{Ker}\phi \approx \boldsymbol{Z}[x]$. Since $U(\boldsymbol{Z}[x]) = \{1, -1\}$ by 1(c), $\boldsymbol{Z}[x]$ is not a field. Hence, $\mathrm{Ker}\phi$ is not a maximal ideal. ■

(d) $\langle y \rangle$ is a prime ideal but not maximal in $R = \boldsymbol{Z}[x, y]$.

Solution. Since every polynomial $f(x, y)$ in $\boldsymbol{Z}[x, y]$ can be written $f_0(x) + f_1(x)y + \cdots + f_n(x)y^n$ for some n. If $f(x, y) \in \mathrm{Ker}\phi$, then $f_0(x) = 0$ and $\mathrm{Ker}\phi = \langle y \rangle$. Thus the assertion follows from (c). ■

(e) $\boldsymbol{Z}[x, y]$ is not a principal ideal domain.

Solution. In a principal ideal domain, every irreducible element generates a maximal ideal. $y \in \boldsymbol{Z}[x, y]$ is irreducible, however $\langle y \rangle$ is not a maximal ideal.■

You can also argue that for example $\langle x, y \rangle$ is not a principal ideal by showing that $\langle x, y \rangle = \langle f(x, y) \rangle$ for some $f(x, y) \in \boldsymbol{Z}[x, y]$ is impossible.

4. Let $R = \{a + b\sqrt{-3} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$ and $\gamma = 1 + \sqrt{-3} \in R$, where $\boldsymbol{C}$ is the complex number field. Show the following. (25pts)

(a) R is an integral domain.

Solution. Let $\phi : \boldsymbol{Z}[x] \to \boldsymbol{C}\ (f(x) \mapsto f(\sqrt{-3}))$. Then the image of this ring homomorphism $\boldsymbol{Z}[\sqrt{-3}]$ is a subring of $\boldsymbol{C}$ containing R. In particular, it is an integral domain. Let $f(x) \in \boldsymbol{Z}[x]$ and write $f(x) = q(x)(x^2 + 3) + a + bx$. This is possible as $x^2 + 3$ is monic. Since $f(\sqrt{-3}) = a + b\sqrt{-3} \in R$, $R = \boldsymbol{Z}[\sqrt{-3}]$ and R is an integral domain. ■

(b) $U(R) = \{1, -1\}$.

Solution. Let $N : R \to \boldsymbol{Z}$ $(a + b\sqrt{-3} \mapsto a + 3b^2 = (a + b\sqrt{-3})(a - b\sqrt{-3}))$. Then for $\alpha, \beta \in R$, $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$. Now, if $\alpha\beta = 1$, then $1 = N(\alpha)N(\beta)$. So if $\alpha = a + b\sqrt{-3}$, $N(\alpha) = 1 = a^2 + 3b^2$. Hence $U(R) \subset \{1, -1\}$. The other inclusion is clear. ■

(c) γ is an irreducible element.

Solution. Suppose $\gamma = \alpha\beta$. Then $4 = N(1 + \sqrt{-3}) = N(\gamma) = N(\alpha)N(\beta)$. If $N(\alpha), N(\beta) \neq 1$, $N(\alpha) = N(\beta) = 2$, which is impossible as $a^2 + 3b^2 \neq 2$ for any integers a and b. Thus, $N(\alpha) = 1$ or $N(\beta) = 1$ and α or $\beta \in U(R)$. ■

(d) $\langle\gamma\rangle$ is not a prime ideal.

Solution. $2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}) \in \langle\gamma\rangle$. However, $2 \notin \langle\gamma\rangle$. As otherwise, $2 = \alpha\gamma$ for some $\alpha \in R$. Since $N(2) = N(\gamma)$, $N(\alpha) = 1$ and $\alpha = \pm 1$, which is impossible. ■

(e) R is not a unique factorization domain.

Solution. In a unique factorization, every irreducible element generates a prime ideal. This is not the case by (c) and (d). ■

You can also argue that $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ and 2, $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are mutually non associative irreducible elements. Hence, the uniqueness of factorization fails.