November 15, 2013

Algebra II Final 2013

If R is a commutative ring with unity 1, then $U(R)$ denotes the set of units, i.e., invertible elements. In an integral domain D, a non-zero non-unit element $\alpha \in D$ is irreducible if $\alpha = \beta\gamma$ with $\beta, \gamma \in D$ implies $\beta \in U(D)$ or $\gamma \in U(D)$. For $a_1, a_2, \ldots, a_n \in R$, $\langle a_1, a_2, \ldots, a_n \rangle$ denotes the smallest ideal of R containing $a_1, a_2, \ldots, a_n$. Then

$$\langle a_1, a_2, \ldots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

When you quote a theorem, state it clearly. You may quote the following facts, if necessary.

I. If R is an integral domain, then

(a) the polynomial ring $R[x]$ over R is an integral domain;

(b) the unit group $U(R[x]) = U(R)$.

II. Let F be a field and $F[x]$ the polynomial ring over F.

(a) $F[x]$ is a principal ideal domain.

(b) Let I be a nonzero ideal in $F[x]$. Let $h(x)$ is a monic[1] nonzero polynomial in I of smallest degree. Then $I = \langle h(x) \rangle$.

Problems

1. Let $x^2 - 2, x^2 + 2$ be polynomials in $\boldsymbol{Q}[x]$. Show the following. (15pts)

(a) $\boldsymbol{Q}[x] = \langle x^2 - 2, x^2 + 2 \rangle$ and $\langle x^2 - 2 \rangle \cap \langle x^2 + 2 \rangle = \langle x^4 - 4 \rangle$.

(b) Let

$$\varphi : \boldsymbol{Q}[x] \to \boldsymbol{Q}[x]/\langle x^2 - 2 \rangle \oplus \boldsymbol{Q}[x]/\langle x^2 + 2 \rangle \quad (f(x) \mapsto (f(x) + \langle x^2 - 2 \rangle, f(x) + \langle x^2 + 2 \rangle)).$$

Then φ is an <u>onto</u> ring homomorphism and $\mathrm{Ker}\varphi = \langle x^4 - 4 \rangle$.

(c) Both $\boldsymbol{Q}[x]/\langle x^2 - 2 \rangle$ and $\boldsymbol{Q}[x]/\langle x^2 + 2 \rangle$ are fields, but $\boldsymbol{Q}[x]/\langle x^4 - 4 \rangle$ is not a field.

[1] the leading coefficient is 1

2. Prove the following. (25pts)

   (a) Find a commutative ring R with unity 1 such that the polynomial ring $R[x]$ does <u>not</u> satisfy $U(R[x]) = U(R)$.

   (b) $\boldsymbol{Z}[x, y]$ is an integral domain, and $U(\boldsymbol{Z}[x, y]) = \{-1, 1\}$.

   (c) Let $f(x, y), g(x, y) \in \boldsymbol{Z}[x, y]$. If $\langle f(x, y)\rangle = \langle g(x, y)\rangle$, then $f(x, y) = \pm g(x, y)$.

   (d) $\langle x, y\rangle$ is not a maximal ideal.

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

3. Let $R = \{a + b\sqrt{-13} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and let $N(a + b\sqrt{-13}) = a^2 + 13b^2$. Show the following. (30pts)

   (a) R is an integral domain and $R = \{f(\sqrt{-13}) \mid f(t) \in \boldsymbol{Z}[t]\}$.

   (b) $U(R) = \{-1, 1\}$, and $\alpha \in R$ is a unit if and only if $N(\alpha) = 1$.

   (c) Four elements $2, 7, 1 - \sqrt{-13}$ and $1 + \sqrt{-13}$ of R are irreducible elements of R.

   (d) R is not a unique factorization domain.

4. Let E be an extension field of F. Let $p(x)$ be an irreducible polynomial of degree n in $F[x]$, and α a zero of $p(x)$ in E. Let $\psi : F[x] \to E$ $(f(x) \mapsto f(\alpha))$. Show the following. (30pts)

   (a) $\mathrm{Ker}\psi = \langle p(x)\rangle$, and $\mathrm{Im}\psi = F(\alpha)$ is the smallest subfield of E containing F and α.

   (b) $[F(\alpha) : F]$, the dimension of $F(\alpha)$ as a vector space over F, is equal to n, the degree of $p(x)$.

   (c) Every element $\beta \in F(\alpha)$ is algebraic over F, i.e.. β is a zero of a nonzero polynomial $q(x) \in F[x]$.

   (d) Suppose $\gamma \in E$ is algebraic over $F(\alpha)$. Then γ is algebraic over F.

November 15, 2013

Solutions to Algebra II Final 2013

1. Let x^2-2, x^2+2 be polynomials in $\boldsymbol{Q}[x]$. Show the following. (15pts)

   (a) $\boldsymbol{Q}[x] = \langle x^2-2, x^2+2\rangle$ and $\langle x^2-2\rangle \cap \langle x^2+2\rangle = \langle x^4-4\rangle$.
   Solution. Since $1 = \frac{1}{4}(x^2+2) - \frac{1}{4}(x^2-2) \in \langle x^2-2, x^2+2\rangle$, for any $f(x) \in \boldsymbol{Q}[x]$, $f(x) = f(x)\cdot 1 \in \langle x^2-2, x^2+2\rangle$. Thus $\boldsymbol{Q}[x] = \langle x^2-2, x^2+2\rangle$.
   Since $x^4-4 = (x^2-2)(x^2+2)$, $\langle x^2-2\rangle \cap \langle x^2+2\rangle \supset \langle x^4-4\rangle$.
   Let $h(x) \in \langle x^2-2\rangle \cap \langle x^2+2\rangle$. Then $h(x) = f(x)(x^2-2) = g(x)(x^2+2)$ for some $f(x), g(x) \in \boldsymbol{Q}[x]$. Now

$$\begin{aligned} h(x) &= h(x)\cdot 1 = \frac{1}{4}h(x)(x^2+2) - \frac{1}{4}h(x)(x^2-2) \\ &= \frac{1}{4}f(x)(x^2-2)(x^2+2) - \frac{1}{4}g(x)(x^2+2)(x^2-2) \in \langle x^4-4\rangle. \quad \blacksquare \end{aligned}$$

   (b) Let

$$\varphi : \boldsymbol{Q}[x] \to \boldsymbol{Q}[x]/\langle x^2-2\rangle \oplus \boldsymbol{Q}[x]/\langle x^2+2\rangle \ (f(x) \mapsto (f(x)+\langle x^2-2\rangle, f(x)+\langle x^2+2\rangle)).$$

   Then φ is an <u>onto</u> ring homomorphism and $\mathrm{Ker}\varphi = \langle x^4-4\rangle$.
   Solution. φ is clearly a ring homomorphism. Since $\mathrm{Ker}\varphi = \langle x^2-2\rangle \cap \langle x^2+2\rangle = \langle x^4-4\rangle$, it suffices to show φ is onto. Let $f(x), g(x) \in \boldsymbol{Q}[x]$. Then

$$\begin{aligned} &\varphi(\frac{1}{4}f(x)(x^2+2) - \frac{1}{4}g(x)(x^2-2)) \\ &= (\frac{1}{4}f(x)(x^2+2) + \langle x^2-2\rangle, -\frac{1}{4}g(x)(x^2-2) + \langle x^2+2\rangle) \\ &= ((1+\frac{1}{4}(x^2-2))f(x) + \langle x^2-2\rangle, (1-\frac{1}{4}(x^2+2))g(x) + \langle x^2+2\rangle) \\ &= (f(x) + \langle x^2-2\rangle, g(x) + \langle x^2+2\rangle). \end{aligned}$$

   Therefore φ is an onto ring homomorphism. $\blacksquare$

   (c) Both $\boldsymbol{Q}[x]/\langle x^2-2\rangle$ and $\boldsymbol{Q}[x]/\langle x^2+2\rangle$ are fields, but $\boldsymbol{Q}[x]/\langle x^4-4\rangle$ is not a field.
   Solution. x^2-2 and x^2+2 are irreducible over $\boldsymbol{Q}$ as $\pm\sqrt{2}, \pm\sqrt{-2} \notin \boldsymbol{Q}$. (One can also apply the Eisenstein's criterion and the Gauss' lemma.) Since $\boldsymbol{Q}[x]$ is a principal ideal domain, every irreducible polynomial generates a maximal ideal. Hence both $\boldsymbol{Q}[x]/\langle x^2-2\rangle$ and $\boldsymbol{Q}[x]/\langle x^2+2\rangle$ are fields. Since $\langle x^4-4\rangle$ is properly contained in $\langle x^2-2\rangle$, $\langle x^4-4\rangle$ is not a maximal ideal. Hence $\boldsymbol{Q}[x]/\langle x^4-4\rangle$ is not a field. $\blacksquare$

2. Prove the following. (25pts)

   (a) Find a commutative ring R with unity 1 such that the polynomial ring $R[x]$ does <u>not</u> satisfy $U(R[x]) = U(R)$.
   Solution. Let $R = \boldsymbol{Z}_4$. Since $(2x+1)(-2x+1) = 1$, $2x+1 \in U(\boldsymbol{Z}_4[x])$. Clealy $2x+1 \notin U(\boldsymbol{Z}_4)$. $\blacksquare$

(b) $\boldsymbol{Z}[x, y]$ is an integral domain, and $U(\boldsymbol{Z}[x, y]) = \{-1, 1\}$.

Solution. Since $\boldsymbol{Z}$ is an integral domain, $\boldsymbol{Z}[x]$ is an integral domain by I (a). Thus again by the same result, $\boldsymbol{Z}[x, y] = (\boldsymbol{Z}[x])[y]$ is an integral domain. Now by I (b), $U(\boldsymbol{Z}[x, y]) = U((\boldsymbol{Z}[x])[y]) = U(\boldsymbol{Z}[x]) = U(\boldsymbol{Z}) = \{1, -1\}$. ■

(c) Let $f(x, y), g(x, y) \in \boldsymbol{Z}[x, y]$. If $\langle f(x, y)\rangle = \langle g(x, y)\rangle$, then $f(x, y) = \pm g(x, y)$.

Solution. If $f(x, y)$ or $g(x, y)$ is zero, both are zero and the assertion is clear. Since $f(x, y) \in \langle g(x, y)\rangle$, there exists $h(x, y) \in \boldsymbol{Z}[x, y]$ such that $f(x, y) = h(x, y)g(x, y)$. Similarly, since $g(x, y) \in \langle f(x, y)\rangle$, there exists $k(x, y) \in \boldsymbol{Z}[x, y]$ such that $g(x, y) = k(x, y)f(x, y)$. Then

$$f(x, y) = h(x, y)g(x, y) = h(x, y)k(x, y)f(x, y).$$

So $f(x, y)(1 - h(x, y)k(x, y)) = 0$. Since $f(x, y) \neq 0$, $h(x, y)k(x, y) = 1$ and $h(x, y) \in U(\boldsymbol{Z}[x, y]) = \{1, -1\}$. Therefore $f(x, y) = \pm g(x, y)$. ■

(d) $\langle x, y\rangle$ is not a maximal ideal.

Solution. Let $\pi : \boldsymbol{Z}[x, y] \to \boldsymbol{Z}$ $(f(x, y) \mapsto f(0, 0))$. Then π is onto. Moreover, $\mathrm{Ker}\pi \supset \langle x, y\rangle$ and $\mathrm{Ker}\pi \cap \boldsymbol{Z} = \{0\}$. Hence $\mathrm{Ker}\pi = \langle x, y\rangle$. Therefore $\boldsymbol{Z}[x, y]/\langle x, y\rangle \approx \boldsymbol{Z}$. Since $\boldsymbol{Z}$ is not a field, $\langle x, y\rangle$ is not a maximal ideal. ■

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

Solution. Suppose $\langle x, y\rangle = \langle h(x, y)\rangle$. Since $x = h(x, y)f(x, y)$ and $y = h(x, y)g(x, y)$ for some $f(x, y), g(x, y) \in \boldsymbol{Z}[x, y]$, $h(x, y) = h \in \boldsymbol{Z}$ by considering the degree of $h(x, y)$ in x and y. This is a contradition as $\langle x, y\rangle \neq \boldsymbol{Z}[x, y]$. Note that $\langle x, y\rangle = \{f(x, y)x + g(x, y)y \mid f(x, y), g(x, y) \in \boldsymbol{Z}[x, y]\}$. ■

3. Let $R = \{a + b\sqrt{-13} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and let $N(a + b\sqrt{-13}) = a^2 + 13b^2$. Show the following. (30pts)

(a) R is an integral domain and $R = \{f(\sqrt{-13}) \mid f(t) \in \boldsymbol{Z}[t]\}$.

Solution. Let $\phi : \boldsymbol{Z}[t] \to \boldsymbol{C}$ $(f(t) \mapsto f(\sqrt{-13}))$. Then clearly ϕ is a nonzero ring homomorphism and $\phi(1) = 1$. So $\mathrm{Im}\phi = \{f(\sqrt{-13}) \mid f(t) \in \boldsymbol{Z}[t]\}$ is a subring of $\boldsymbol{C}$. Since $\boldsymbol{C}$ is a field, there is no zero-divisor and $\mathrm{Im}\phi$ is an integral domain. Thus it remains to show that $\mathrm{Im}\phi = R$. Since $a + b\sqrt{-13} = \phi(a + bt)$, $\mathrm{Im}\phi \supset R$. Let $f(t) \in \boldsymbol{Z}[t]$. Then there exist $q(t) \in \boldsymbol{Z}[t]$ and $a, b \in \boldsymbol{Z}$ such that $f(t) = q(t)(x^2+13)+a+bt$ as x^2+13 is a monic polynomial of degree 2. Now $\phi(f(t)) = f(\sqrt{-13}) = a+b\sqrt{-13} \in R$. ■

(b) $U(R) = \{-1, 1\}$, and $\alpha \in R$ is a unit if and only if $N(\alpha) = 1$.

Solution. Since $N(\alpha) = \alpha \cdot \overline{\alpha}$, $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$. Suppose $\alpha\beta = 1$. Then $1 = N(1) = N(\alpha)N(\beta)$. Since $N(\alpha), N(\beta)$ are nonnegative integers by definition, $N(\alpha) = 1$. Conversely if $N(\alpha) = 1$, then $\overline{\alpha} = \alpha^{-1}$. Let $\alpha = a + b\sqrt{-13}$ with $a, b \in \boldsymbol{Z}$. If $N(\alpha) = 1$, then $a^2 + 13b^2 = 1$. The only possibilities are $\alpha = \pm 1$. Since $1, -1$ are units, this prove assertions. ■

(c) Four elements $2, 7, 1 - \sqrt{-13}$ and $1 + \sqrt{-13}$ of R are irreducible elements of R.

Solution. Let $\alpha \in \{2, 7, 1 - \sqrt{-13}, 1 + \sqrt{-13}\}$. Then $N(\alpha) \in \{4, 49, 14\}$. Since $2, 7$ cannot be expressed as $a^2 + 13b^2$ for some $a, b \in \boldsymbol{Z}$, α is irreducible. Note that if $\alpha = \beta\gamma$ with $N(\beta) \neq 1$, $N(\gamma) \neq 1$, then $N(\alpha) = N(\beta)N(\gamma)$ and $N(\beta), N(\gamma) \in \{2, 7\}$. ■

(d) R is not a unique factorization domain.

Solution. By the previous problem, $2, 7, 1-\sqrt{-13}$ and $1+\sqrt{-13}$ of R are irreducible elements of R. Since

$$2 \cdot 7 = 14 = (1-\sqrt{-13})(1+\sqrt{-13}),$$

the decomposition is not unique. Note that it is easy to see that 2 is not an associate of $1 \pm \sqrt{-13}$ as the value of N is not equal. ■

4. Let E be an extension field of F. Let $p(x)$ be an irreducible polynomial of degree n in $F[x]$, and α a zero of $p(x)$ in E. Let $\psi : F[x] \to E$ ($f(x) \mapsto f(\alpha)$). Show the following. (30pts)

(a) $\mathrm{Ker}\psi = \langle p(x) \rangle$, and $\mathrm{Im}\psi = F(\alpha)$ is the smallest subfield of E containing F and α.

Solution. Since $p(\alpha) = 0$, $\langle p(x) \rangle \subset \mathrm{Ker}\psi$. Since $F[x]$ is a principal ideal domain and $p(x)$ an irreducible element, $\langle p(x) \rangle$ is a maximal ideal. Since $\psi(1) = 1$, ψ is not a zero mapping, $\mathrm{Ker}\psi \neq F[x]$. Hence $\mathrm{Ker}\psi = \langle p(x) \rangle$. Thus by an isomorphism theorem, $F[x]/\mathrm{Ker}\psi \approx \mathrm{Im}\psi \subset F(\alpha)$ and $\mathrm{Im}\psi$ is a field containing F and α. Therefore, $\mathrm{Im}\psi = F(\alpha)$. ■

(b) $[F(\alpha) : F]$, the dimension of $F(\alpha)$ as a vector space over F, is equal to n, the degree of $p(x)$.

Solution. Let $f(x) \in F[x]$. Then there exist $q(x), r(x) \in F[x]$ such that $f(x) = q(x)p(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < n$. Since $f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$. $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}$. Now it suffices to show that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent. Suppose $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$ for some $a_0, a_1, \ldots, a_{n-1} \in F$. Let $q(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F[x]$. This implies $q(x) = 0$, as $p(x)$ is of smallest degree among nonzero polynomials in $\langle p(x) \rangle = \mathrm{Ker}\psi$. ■

(c) Every element $\beta \in F(\alpha)$ is algebraic over F, i.e.. β is a zero of a nonzero polynomial $q(x) \in F[x]$.

Solution. Since $[F(\alpha) : F] = n$, the set $\{1, \beta, \beta^2, \ldots, \beta^n\}$ is linearly dependent. Hence there exist $c_0, c_1, \ldots, c_n \in F$ not all zero such that $q(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n \neq 0$ satisfies $q(\beta) = 0$. ■

(d) Suppose $\gamma \in E$ is algebraic over $F(\alpha)$. Then γ is algebraic over F.

Solution. Let $q(x)$ be the minimal polynomial of γ over $F(\alpha)$. Then $[F(\alpha, \gamma) : F(\alpha)] = \deg q(x)$. Hence

$$[F(\alpha, \gamma) : F] = [F(\alpha, \gamma) : F(\alpha)][F(\alpha) : F] = \deg q(x) \deg p(x) < \infty.$$

Let $m = \deg q(x) \deg p(x)$. Then $1, \gamma, \gamma^2, \ldots, \gamma^m$ is linearly dependent over F, and we can find a nonzero polynomial $f(x) \in F[x]$ of degree at most m, such that $f(\gamma) = 0$ by the same argument employed in the previous problem. Hence γ is algebraic over F. ■

Hiroshi Suzki @ International Christian University