November 14, 2014

Algebra II Final 2014

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 apply 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 $n = 135 = 5 \cdot 3^3$. For $\boldsymbol{Z}_{135}$, show the following. (25pts)

  (a) How many zero divisors are there in $\boldsymbol{Z}_{135}$? Show that $\boldsymbol{Z}_{135}$ is not a field.

  (b) Show that $\boldsymbol{Z}_{135} \approx \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$.
  (Consider: $\phi : \boldsymbol{Z} \to \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}\, (m \mapsto (m \pmod 5), m \pmod{27}))$. You may use the fact that $\boldsymbol{Z}/n\boldsymbol{Z} \approx \boldsymbol{Z}_n$.)

  (c) Show that any ideal A of $\boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$ is a principal ideal, i.e, there exists $a \in \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$ such that $A = \langle a \rangle$.

  (d) Find all idempotents e such that with $e^2 = e$ in $\boldsymbol{Z}_{135}$, and corresponding elements in $\boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$.

  (e) Find all ring homomorphisms from $\boldsymbol{Z}_{135}$ to itself.

[1] the leading coefficient is 1

2. Let $R = \boldsymbol{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and $R[x]$ polynomial ring over R. Prove the following. You may assume that R is a subring of $\boldsymbol{C}$ and is a principal ideal domain. (25pts)

   (a) Show that $U(R) = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$.

   (b) Let $\alpha = a + b\sqrt{-1}$. If $a^2 + b^2$ is a prime number, then α is irreducible.

   (c) Let $f(x), g(x) \in R[x]$ and let $A = \langle f(x) \rangle$ and $B = \langle g(x) \rangle$ be ideals of $R[x]$. Show that $A = B$ if and only if there exists $u \in U(R)$ such that $f(x) = u \cdot g(x)$.

   (d) x is an irreducible element in $R[x]$.

   (e) $R[x]$ is not a principal ideal domain.

3. Let $R = \{a + b\sqrt{-17} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and let $N(a + b\sqrt{-17}) = a^2 + 17b^2$. Show the following. (25pts)

   (a) R is a subring of $\boldsymbol{C}$.

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

   (c) 2 is an irreducible element of R.

   (d) $\langle 2 \rangle$ is not a prime ideal of R.

   (e) R is not a unique factorization domain.

4. Let $\sqrt[3]{2}$ be a root of $x^3 - 2$ in $\boldsymbol{R}$. Let $\psi : \boldsymbol{Q}[x] \to \boldsymbol{C}$ $(f(x) \mapsto f(\sqrt[3]{2}))$. Show the following. (25pts)

   (a) Find a prime number p such that $x^3 - 2 \in \boldsymbol{Z}_p[x]$ is irreducible.

   (b) $\mathrm{Ker}(\psi) = \langle x^3 - 2 \rangle$.

   (c) $\mathrm{Im}(\psi) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \boldsymbol{Q}\}$.

   (d) $\mathrm{Im}(\psi)$ is a field.

   (e) Find the splitting field of $x^3 - 2$ in $\boldsymbol{C}$.

Solutions to Algebra II Final 2014

1. Let $n = 135 = 5 \cdot 3^3$. For $\boldsymbol{Z}_{135}$, show the following. (25pts)

   (a) How many zero divisors are there in $\boldsymbol{Z}_{135}$? Show that $\boldsymbol{Z}_{135}$ is not a field.
   Solution. There are $\varphi(135) = \varphi(3^3 \cdot 5) = 3^2(3-1)(5-1) = 2^3 \cdot 3^2 = 72$ units, which are nonnegative integers at most 134 which are coprime to 135. Since all nonzero non-unit elements are zero divisors in a finite commutative ring with 1, there are $135 - 72 - 1 = 62$ zero devisors. Since a field does not have a zero divisor, $\boldsymbol{Z}_{135}$ is not a field. ■

   (b) Show that $\boldsymbol{Z}_{135} \approx \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$.
   (Consider: $\phi : \boldsymbol{Z} \to \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}\,(m \mapsto (m \pmod 5), m \pmod{27}))$. You may use the fact that $\boldsymbol{Z}/n\boldsymbol{Z} \approx \boldsymbol{Z}_n$.)
   Solution. $\mathrm{Ker}\phi = 5\boldsymbol{Z} \cap 27\boldsymbol{Z} = 135\boldsymbol{Z}$ as 5 and 27 are cop rime. So $\boldsymbol{Z}/135\boldsymbol{Z}$ is isomorphic to a subring of $\boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$ by isomorphism theorem. Since

   $$135 = |\boldsymbol{Z}/135\boldsymbol{Z}| = |\phi(\boldsymbol{Z}/135\boldsymbol{Z})| \leq |\boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}| = 135,$$

   ϕ is onto. Therefore $\boldsymbol{Z}_{135} \approx \boldsymbol{Z}/135\boldsymbol{Z} \approx \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$. ■

   (c) Show that any ideal A of $\boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$ is a principal ideal, i.e, there exists $a \in \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$ such that $A = \langle a \rangle$.
   Solution. Since $\boldsymbol{Z}_{135}$ is cyclic, its Abelian subgroups are cyclic. Since every ideal is a subgroup, it is generated by a single element, and it can be written as $\langle a \rangle$ for some $a \in \boldsymbol{Z}_{135}$. Hence, every ideal of $\boldsymbol{Z}_{135}$ is a principal ideal. ■

   (d) Find all idempotents e such that with $e^2 = e$ in $\boldsymbol{Z}_{135}$, and corresponding elements in $\boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{27}$.
   Solution. In $\boldsymbol{Z}_5$ and $\boldsymbol{Z}_{27}$, 0 and 1 are the only idempotents. Note that $0 = e^2 - e = e(e-1)$ and if e is an integer, p^n divides $e(e-1)$ if and only if $p^n \mid e$ or $p^n \mid e - 1$. Hence, $0 \leftrightarrow (0,0)$, $1 \leftrightarrow (1,1)$, $81 \leftrightarrow (1,0)$, and $55 \leftrightarrow (0,1)$ are the only idempotents. ■

   (e) Find all ring homomorphisms from $\boldsymbol{Z}_{135}$ to itself.
   Solution. Since $\phi(1) = \phi(1 \cdot 1) = \phi(1)^2$, $\phi(1)$ is an idempotent. Hence $\phi(1) \in \{0, 1, 55.81\}$. Therefore, $\phi(n) = n\phi(0)$, and $\phi(x) = 0$, x, $55x$ or $81x$. Conversely, these are ring homomorphisms. ■

2. Let $R = \boldsymbol{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and $R[x]$ polynomial ring over R. Prove the following. You may assume that R is a subring of $\boldsymbol{C}$ and is a principal ideal domain. (25pts)

(a) Show that $U(R) = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$.

Solution. It is clear that $U(R) \supset \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$. Let $\alpha = a + b\sqrt{-1} \in R[\sqrt{-1}]$. First claim that $\alpha \in U(R)$ iff $N(\alpha) = 1$, where $N(\alpha) = a^2 + b^2$. If $N(\alpha) = 1$, then $(a + b\sqrt{-1})(a - b\sqrt{-1}) = 1$, and $a - b\sqrt{-1} = (a + b\sqrt{-1})^{-1}$. Thus $\alpha \in U(R)$. Conversely, suppose $\alpha \in U(R)$. Then there exists $\beta \in R$ such that $\alpha\beta = 1$. Now $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$. Since $N(\alpha) = a^2 + b^2$, $N(\alpha)$ is a positive integer. Hence $N(\alpha) = 1$. Now it is clear that $a^2 + b^2 = 1$ implies that $\alpha = a + b\sqrt{-1} = 1, -1, \sqrt{-1}$, or $-\sqrt{-1}$. ■

(b) Let $\alpha = a + b\sqrt{-1}$. If $a^2 + b^2$ is a prime number, then α is irreducible.

Solution. Suppose $N(\alpha) = a^2 + b^2 = p$, and $\alpha = \beta\gamma$ for some $\beta, \gamma \in R$. Then $p = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Since $N(\beta)$ and $N(\gamma)$ are nonnegative integers and p a prime, either $N(\beta) = 1$ or $N(\gamma) = 1$. As we showed in (a), $\beta \in U(R)$ or $\gamma \in U(R)$. ■

(c) Let $f(x), g(x) \in R[x]$ and let $A = \langle f(x) \rangle$ and $B = \langle g(x) \rangle$ be ideals of $R[x]$. Show that $A = B$ if and only if there exists $u \in U(R)$ such that $f(x) = u \cdot g(x)$.

Solution. First note by I (b) that $U(R[x]) = U(R)$ as $R \subset \boldsymbol{C}$ is an integral domain. Suppose $A = B$. If $A = B = \{0\}$, then $f(x) = g(x) = 0$ and we can take $u = 1 \in U(R)$. Assume that $A = B \neq \{0\}$. In particular, $f(x) \neq 0 \neq g(x)$. Then $f(x) \in \langle f(x) \rangle = A = B = \langle g(x) \rangle \ni g(x)$. Hence there exist $h(x), k(x) \in R[x]$ such that $f(x) = h(x)g(x)$ and $g(x) = k(x)f(x)$. Therefore,

$$0 = f(x) - h(x)g(x) = f(x) - h(x)k(x)f(x) = (1 - h(x)k(x))f(x).$$

Since $R[x]$ is an integral domain and $f(x) \neq 0$, $1 = h(x)k(x)$ and $h(x) \in U(R[x]) = U(R)$. Since $f(x) = h(x)g(x)$, there exists $u \in U(R)$ such that $f(x) = u \cdot g(x)$.

Conversely, suppose there exists $u \in U(R)$ such that $f(x) = u \cdot g(x)$. Then

$$\langle f(x) \rangle = \langle u \cdot g(x) \rangle \subset \langle g(x) \rangle = \langle u^{-1} \cdot f(x) \rangle \subset \langle f(x) \rangle,$$

and $A = \langle f(x) \rangle = \langle g(x) \rangle = B$. ■

(d) x is an irreducible element in $R[x]$.

Solution. Suppose $x = u(x)v(x)$. Then comparing degrees, either $u(x)$ or $v(x)$ is a nonzero constant, and the other is of degree 1. Let $u(x) = u \in R$. Since $0 = uv(0)$, $v(0) = 0$ and $v(x) = vx$ for some nonzero constant $v \in R$. Thus $x = uvx$ and $u \in U(R) = U(R[x])$. Therefore, x is irreducible. ■

(e) $R[x]$ is not a principal ideal domain.

Solution. Let $\pi : R[x] \to R$ $(f(x) \mapsto f(0))$. Then π is a ring homomorphism and $\mathrm{Ker}\pi = \langle x \rangle$. Since π is onto, $R[x]/\langle x \rangle \approx R$. Suppose $R[x]$ is a principal ideal domain. Since x is an irreducible element in a principal ideal domain, $\langle x \rangle$ is a maximal ideal and $R[x]/\langle x \rangle \approx R$ is a field. Since $U(R) = \{1, -1, \sqrt{-1}, -\sqrt{-1}\} \neq R \setminus \{0\}$, R is not a field, a contradiction. ■

3. Let $R = \{a + b\sqrt{-17} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and let $N(a + b\sqrt{-17}) = a^2 + 17b^2$. Show the following. (25pts)

   (a) R is a subring of $\boldsymbol{C}$.

   Solution. For all $a, b, c, d \in \boldsymbol{R}$, $(a + b\sqrt{-17}) - (c + d\sqrt{-17}) = (a - c) + (b - d)\sqrt{-17}$, and $(a + b\sqrt{-17})(c + d\sqrt{-17}) = ac - 17bd + (ad + bc)\sqrt{-17} \in R$ as $ac - 17cd, ad + bd \in R$. Hence R is a subring of $\boldsymbol{C}$. ■

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

   Solution. Suppose $\alpha = a + b\sqrt{-17} \in U(R)$. Then there exists $\beta \in U(R)$ such that $\alpha\beta = 1$. As $1 = N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(\alpha)$ is a nonnegative integer, $N(\alpha) = 1$. Conversely if $N(\alpha) = 1$, then $(a+b\sqrt{-17})(a-b\sqrt{-17}) = 1$ and $\alpha = a + b\sqrt{-17} \in U(R)$. Now it is clear that $\{1, -1\} \subset U(R)$ and $a^2 + 17b^2 = N(\alpha) = 1$ if and only if $\alpha = \pm 1$. ■

   (c) 2 is an irreducible element of R.

   Solution. Suppose $2 = \alpha\beta$ with $\alpha, \beta \in R$. Then $4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$. So if $N(\alpha) \neq 1 \neq N(\beta)$, then $N(\alpha) = N(\beta) = 2$, which is absurd as $N(\alpha) = a^2 + 17b^2$ cannot express 2 when $a, b \in \boldsymbol{Z}$. Therefore, $N(\alpha) = 1$ or $N(\beta) = 1$ and $\alpha \in U(R)$ or $\beta \in U(R)$ as shown in (b). ■

   (d) $\langle 2 \rangle$ is not a prime ideal of R.

   Solution. $(1 + \sqrt{-17})(1 - \sqrt{-17}) = 18 \in \langle 2 \rangle$. However, if $1 \pm \sqrt{-17} = 2\alpha$, then $18 = N(1 \pm \sqrt{-17}) = N(2)N(\alpha) = 4N(\alpha)$. This is a contradiction as $N(\alpha)$ is an integer. ■

   (e) R is not a unique factorization domain.

   Solution. If R is a unique factorization domain, every irreducible element generates a prime ideal. By (d), this is not the case. ■

4. Let $\sqrt[3]{2}$ be a root of $x^3 - 2$ in $\boldsymbol{R}$. Let $\psi : \boldsymbol{Q}[x] \to \boldsymbol{C}$ $(f(x) \mapsto f(\sqrt[3]{2}))$. Show the following. (25pts)

   (a) Find a prime number p such that $x^3 - 2 \in \boldsymbol{Z}_p[x]$ is irreducible.

   Solution. We claim that $x^3 - 2 \in \boldsymbol{Z}_7[x]$ is irreducible. Since $x^3 - 2$ is of degree three, it suffices to show that $x^3 - 2$ does not have a zero in $\boldsymbol{Z}_7$. Since $\{a^3 \mid a \in \boldsymbol{Z}_7\} = \{0, 1, 6\}$, $x^3 - 2$ does not have a zero in $\boldsymbol{Z}_7$ and $x^3 - 2$ is irreducible. ■

   (b) $\mathrm{Ker}(\psi) = \langle x^3 - 2 \rangle$.

   Solution. First by (a), $x^3 - 2$ is irreducible over $\boldsymbol{Z}$ and so it is irreducible over $\boldsymbol{Q}$ by Gauss' lemma. Clearly, $x^3 - 2 \in \mathrm{Ker}(\psi)$. Since $\boldsymbol{Q}[x]$ is a polynomial ring over a field, it is a principal ideal domain by II (a). In a principal ideal domain, every irreducible element generates a maximal ideal. $\langle x^3 - 2 \rangle \subset \mathrm{Ker}(\psi)$ implies $\langle x^3 - 2 \rangle = \mathrm{Ker}(\psi)$, as $1 \notin \mathrm{Ker}(\psi)$ and $\mathrm{Ker}(\psi) \neq \boldsymbol{Q}[x]$. ■

(c) $\mathrm{Im}(\psi) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \boldsymbol{Q}\}$.

Solution. Since $\psi(a + bx + cx^2) = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$, $\mathrm{Im}(\psi) \supset \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \boldsymbol{Q}\}$. Let $f(x) \in \boldsymbol{Q}[x]$ and $f(x) = q(x)(x^3-2)+a+bx+cx^2$ for some $q(x) \in \boldsymbol{Q}[x]$ and $a, b, c \in \boldsymbol{Q}$ by division algorithm. Since $\sqrt[3]{2}$ is a zero of $x^3 - 2$, $\psi(f(x)) = f(\sqrt[3]{2}) = a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2$ and $\mathrm{Im}(\psi) \subset \{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2 \mid a, b, c \in \boldsymbol{Q}\}$. ■

(d) $\mathrm{Im}(\psi)$ is a field.

Solution. By isomorphism theorem, $\boldsymbol{Q}[x]/\langle x^3 - 2\rangle = \boldsymbol{Q}[x]/\mathrm{Ker}(\psi) \approx \mathrm{Im}(\psi)$. Since $\langle x^3 - 2\rangle$ is a maximal ideal as stated in (b), $\boldsymbol{Q}[x]/\langle x^3 - 2\rangle$ is a field. Therefore, $\mathrm{Im}(\psi)$ is a field. ■

(e) Find the splitting field of $x^3 - 2$ in $\boldsymbol{C}$.

Solution. Since $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$, zeros are $\sqrt[3]{2}$ and $(-\sqrt[3]{2} \pm \sqrt{\sqrt[3]{2}^2(-3)})/2 = \sqrt[3]{2}(-1 \pm \sqrt{-3})/2$. Therefore, the splitting field is

$$\boldsymbol{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\frac{-1-\sqrt{-3}}{2}, \sqrt[3]{2}\frac{-1+\sqrt{-3}}{2}\right) = \boldsymbol{Q}(\sqrt[3]{2}, \sqrt{-3}).$$

Either expression is fine. ■

Let $\omega = (-1 + \sqrt{-3})/2$. Then $\omega^3 = 1$ and $\omega^2 = (-1 - \sqrt{-3})/2$. So zeros are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$.