November 19, 2010

Algebra II Final 2010

1. Let R be an integral domain. For $a \in R$, $\langle a \rangle = \{ra \mid r \in R\}$. Show the following. (25pts)
   (a) For $a, b \in R$, the following are equivalent.
      (i) $\langle a \rangle = \langle b \rangle$.
      (ii) There exists a unit, i.e., invertible element, $u \in R$ such that $b = ua$.
   (b) The following are equivalent.
      (i) R is a field.
      (ii) For every nonzero $a \in R$, $\langle a \rangle = R$.
   (c) If R has finitely many elements, then R is a field.

2. Let n be an arbitrary positive integer such that $n \geq 2$. Show the following. (15pts)
   (a) If $\phi : \boldsymbol{Z}_n \to \boldsymbol{Z}_n$ is a ring homomorphism, there is $e \in \boldsymbol{Z}_n$ such that $e^2 = e$ and $\phi(a) = ae$.
   (b) If $e \in \boldsymbol{Z}_n$ satisfies $e^2 = e$, then $\phi : \boldsymbol{Z}_n \to \boldsymbol{Z}_n$ $(a \mapsto ae)$ is a ring homomorphism.
   (c) How many ring homomorphisms are there from $\boldsymbol{Z}_{45}$ into $\boldsymbol{Z}_{45}$.

3. Let $R = \{a + b\sqrt{-5} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and let $N(a + b\sqrt{-5}) = a^2 + 5b^2$. (35pts)
   (a) Show that R is an integral domain and $R = \{f(\sqrt{-5}) \mid f(t) \in \boldsymbol{Z}[t]\}$.
   (b) Show that for $\alpha \in R$, $\alpha \in U(R)$ if and only if $N(\alpha) = 1$.
   (c) Show that 2 is an irreducible element.
   (d) Show that $\langle 2 \rangle$ is not a prime ideal.
   (e) Show that R is not a unique factorization domain. (Use only the definition of unique factorization domains.)

4. Let $\alpha \in \boldsymbol{C}$ and let $p(x) \in \boldsymbol{Z}[x]$ a monic irreducible polynomial over $\boldsymbol{Z}$ of degree n such that $p(\alpha) = 0$. We consider a ring homomorphism $\phi : \boldsymbol{Q}[x] \to \boldsymbol{C}$ $(f(x) \mapsto f(\alpha))$. (25pts)
   (a) Show that $\mathrm{Ker}\phi = \langle p(x) \rangle$.
   (b) Show that $\mathrm{Im}\phi$ is a field.
   (c) If $\beta \in \boldsymbol{C}$ satisfies $p(\beta) = 0$, then $\boldsymbol{Q}(\alpha) \approx \boldsymbol{Q}(\beta)$.
   (d) Suppose $q(x) \in \boldsymbol{Q}[x]$ is irreducible over $\boldsymbol{Q}$ of degree m, if $\gcd(n, m) = 1$, then $q(x)$ is irreducible over $\boldsymbol{Q}(\alpha)$.

Solutions to Algebra II Final 2010

1. Let R be an integral domain. For $a \in R$, $\langle a \rangle = \{ra \mid r \in R\}$. Show the following. (25pts)

   (a) For $a, b \in R$, the following are equivalent.

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

   (ii) There exists a unit, i.e., invertible element, $u \in R$ such that $b = ua$.

   Solution. (i)→(ii) Since R has identity, $b = 1b \in \langle b \rangle = \langle a \rangle$. So there is $u \in R$ such that $b = ua$. Similarly, $a = 1a \in \langle a \rangle = \langle b \rangle$, there exists $v \in R$ such that $a = vb$, If $b = 0$, then $a = 0$. So $b = 0 = 1 \cdot 0 = 1 \cdot a$. We may assume that $b \neq 0$. Now $0 = b - b = b - ua = b - uvb = (1 - uv)b$. Since R is an integral domain and $b \neq 0$, $1 = uv$ and u is a unit. Note that integral domains are commutative. ■

   (ii)→(i) Since $b = ua \in \langle a \rangle$, $\langle b \rangle \subset \langle a \rangle$. Since u is a unit, $a = u^{-1}b \in \langle b \rangle$. Hence $\langle a \rangle \subset \langle b \rangle$. Thus $\langle a \rangle = \langle b \rangle$. ■

   (b) The following are equivalent.

   (i) R is a field.

   (ii) For every nonzero $a \in R$, $\langle a \rangle = R$.

   Solution. (i)→(ii) Since R is a field, every nonzero element a is a unit. So a^{-1} is also a unit and $1 = a^{-1}a$. Hence by (a) (ii)→(i), $\langle a \rangle = \langle 1 \rangle = R$. ■

   (ii)→(i) Let a be a nonzero element of R. Then by assumption, $\langle a \rangle = R$. Since $1 \in R$, there is $b \in R$ such that $1 = ba$. Since R is commutative, a is a unit. Since a is arbitrary nonzero element of R, R is a field. ■

   (c) If R has finitely many elements, then R is a field.

   Solution. Let a be a nonzero element of R. Let $\phi : R \to R$ $(x \mapsto xa)$. Since $\phi(x) = \phi(y)$ implies $0 = xa - ya = (x - y)a$ and a is a nonzero element in an integral domain, $x = y$. Thus ϕ is an injection. Since R has finitely many elements, ϕ is a surjection as well. Thus $R = \mathrm{Im}\phi = \{xa \mid x \in R\} = \langle a \rangle$. Now by (b) (ii)→(i), R is a field. ■

2. Let n be an arbitrary positive integer such that $n \geq 2$. Show the following. (15pts)

   (a) If $\phi : \boldsymbol{Z}_n \to \boldsymbol{Z}_n$ is a ring homomorphism, there is $e \in \boldsymbol{Z}_n$ such that $e^2 = e$ and $\phi(a) = ae$.

   Solution. 1 is the identity element in $\boldsymbol{Z}_n$. Let $e = \phi(1)$. Then $e = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = e^2$. Moreover if $a \in \boldsymbol{Z}_n$, then a can be regarded as a nonnegative integer, $\phi(a) = \phi(a1) = a\phi(1) = ae$. Note that $a1$ is the sum of a 1's in $\boldsymbol{Z}_n$. ■

   (b) If $e \in \boldsymbol{Z}_n$ satisfies $e^2 = e$, then $\phi : \boldsymbol{Z}_n \to \boldsymbol{Z}_n$ $(a \mapsto ae)$ is a ring homomorphism.

   Solution. $\phi(a + b) = (a + b)e = ae + be = \phi(a) + \phi(b)$, and $\phi(ab) = abe = abee = aebe = \phi(a)\phi(b)$. Hence ϕ is a ring homomorphism. ■

   (c) How many ring homomorphisms are there from $\boldsymbol{Z}_{45}$ into $\boldsymbol{Z}_{45}$.

   Solution. By (a) and (b), $\phi(1)$ is an idempotent, i.e., an element $e \in \boldsymbol{Z}_n$ such that $e^2 = e$ and for each e, there is a ring homomorphism such that $\phi(1) = e$. Thus there is a one-to-one correspondence between a ring homomorphism from $\boldsymbol{Z}_n$ to itself and an idempotent of $\boldsymbol{Z}_n$. So the number of ring homomorphisms from $\boldsymbol{Z}_{45}$ into $\boldsymbol{Z}_{45}$ is equal to the number of idempotents in $\boldsymbol{Z}_{45}$. Set $f = 1 - e$. Then $f^2 = f$ and since $ef = e(1-e) = 0$, $45 \mid ef$ and e and $f = 1 - e$ are coprime. So if $3 \mid e$, then $9 \mid e$. Thus we may assume that $5 \mid e$ and $9 \mid f$ or $9 \mid e$ and $5 \mid f$. Thus $5x + 9y = 1$ and $e = 5x$ or $e = 9y$. They are $\{0, 1, 10, 36\}$. ■

3. Let $R = \{a + b\sqrt{-5} \mid a, b \in \boldsymbol{Z}\} \subset \boldsymbol{C}$, and let $N(a + b\sqrt{-5}) = a^2 + 5b^2$. (35pts)

   (a) Show that R is an integral domain and $R = \{f(\sqrt{-5}) \mid f(t) \in \boldsymbol{Z}[t]\}$.
   Solution. Let $\phi : \boldsymbol{Z}[t] \to \boldsymbol{C}(f(t) \mapsto f(\sqrt{-5}))$. Let $f(t) \in \boldsymbol{Z}[t]$. Then there exist $q(t)$, $r(t) \in \boldsymbol{Z}[t]$ such that $f(t) = q(t)(t^2 + 5) + r(t)$ with $\deg(r(t)) \leq 1$. Since $\phi(f(t)) = r(\sqrt{-5})$, and $r(t)$ is of degree at most 1, and can be written as $r(t) = a + b\sqrt{-5}$ and $r(\sqrt{-5}) = a + b\sqrt{-5}$ for some $a, b \in \boldsymbol{Z}$.
   $$\mathrm{Im}\phi = \{f(\sqrt{-5}) \mid f(t) \in \boldsymbol{Z}[t]\} = \{r(\sqrt{-5}) \mid r(t) \in \boldsymbol{Z}[t],\ \deg r(t) \leq 1\} = R.$$
   Since $R = \mathrm{Im}\phi$ is a subring of a field $\boldsymbol{C}$ containing 1, it is a commutative ring with identity having no zero divisors. Thus R is an integral domain. ■

   (b) Show that for $\alpha \in R$, $\alpha \in U(R)$ if and only if $N(\alpha) = 1$.
   Solution. Since complex conjugates $\bar{\alpha}, \bar{\beta}$ of $\alpha, \beta \in \boldsymbol{C}$ satisfy $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$ and $N(a + b\sqrt{-5}) = a^2 + 5b^2 = (a + b\sqrt{-5})\overline{(a + b\sqrt{-5})}$, $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta)$. Now if $\alpha \in U(R)$, then there is $\beta \in R$ such that $\alpha\beta = 1$. Hence $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Since both $N(\alpha)$ and $N(\beta)$ are nonnegative integers, $N(\alpha) = 1$. Conversely, if $N(\alpha) = 1$ for $\alpha = a + b\sqrt{-5}$, then $\alpha\bar{\alpha} = N(\alpha) = 1$ and $\bar{\alpha} = a - b\sqrt{-5} \in R$ is the inverse of α and $\alpha \in U(R)$. It is also easy to see that $N(\alpha) = a^2 + 5b^2 = 1$ if and only if $\alpha = \pm 1$. So the converse part is clear. ■

   (c) Show that 2 is an irreducible element.
   Solution. Suppose $2 = \alpha\beta$ with $\alpha, \beta \in R \setminus U(R)$. Then $4 = N(2) = N(\alpha)N(\beta)$ and $N(\alpha) \neq 1$, $N(\beta) \neq 1$ by (b). The only possible case is $N(\alpha) = N(\beta) = 2$. But this is impossible as 2 cannot be expressed as the form $a^2 + 5b^2$ for some integers a, b. Therefore if $2 = \alpha\beta$, either α or β is a unit and 2 is an irreducible element. ■

   (d) Show that $\langle 2 \rangle$ is not a prime ideal.
   Solution. First $1 \pm \sqrt{-5} \in R$ and $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 3 \cdot 2 \in \langle 2 \rangle$. If $1 \pm \sqrt{-5} \in \langle 2 \rangle$, there exists $\alpha \in R$ such that $1 \pm \sqrt{-5} = 2\alpha$. Then $6 = N(1 \pm \sqrt{-5}) = N(2\alpha) = N(2)N(\alpha) = 4N(\alpha)$. Since $N(\alpha)$ is a positive integer, this is impossible. Therefore $1 \pm \sqrt{-5} \notin \langle 2 \rangle$ and $\langle 2 \rangle$ is not a prime ideal. ■

   (e) Show that R is not a unique factorization domain. (Use only the definition of unique factorization domains.)
   Solution. As in the proof of (d), $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, Since 2 is an irreducible element in R, 2 must divide $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$. But it is shown that this is not the case as $1 \pm \sqrt{-5} \notin \langle 2 \rangle$. Therefore, R is not a unique factorization domain. ■

4. Let $\alpha \in \boldsymbol{C}$ and let $p(x) \in \boldsymbol{Z}[x]$ a monic irreducible polynomial over $\boldsymbol{Z}$ of degree n such that $p(\alpha) = 0$. We consider a ring homomorphism $\phi : \boldsymbol{Q}[x] \to \boldsymbol{C}$ $(f(x) \mapsto f(\alpha))$. (25pts)

   (a) Show that $\mathrm{Ker}\phi = \langle p(x) \rangle$.
   Solution. Since $p(x)$ is nonzero, $\mathrm{Ker}\phi \neq 0$ as $p(x) \in \mathrm{Ker}\phi$. By Gauss' lemma, $p(x)$ is irreducible over $\boldsymbol{Q}$.

We claim that $\boldsymbol{Q}[x]$ is a principal ideal domain. Let I be an ideal of $\boldsymbol{Q}[x]$. Since 0 ideal is a principal ideal generated by 0, assume I is nonzero. Let $q(x)$ be a nonzero polynomial in I of least degree. Let $f(x) \in I$ and let $f(x) = g(x)q(x) + r(x)$ with $\deg r(x) < \deg q(x)$. Since $f(x), q(x) \in I$, $r(x) = f(x) - g(x)q(x) \in I$. By the choice of $q(x)$, $r(x) = 0$. So $f(x) \in I$ implies $q(x) \mid f(x)$ and $I = \langle q(x) \rangle$. This shows that $\boldsymbol{Q}[x]$ is a principal ideal domain.

Now we apply the fact for the ideal $\mathrm{Ker}\phi$. If $q(x)$ is a nonzero element of $\mathrm{Ker}\phi$ of least degree, then $q(x) \mid p(x)$ and $q(x)$ is a nonzero constant multiple of $p(x)$ as $p(x)$ is irreducible over $\boldsymbol{Q}$, and $p(x)$ has the same property as $q(x)$. Thus $\mathrm{Ker}\phi = \langle p(x) \rangle$. ■

(b) Show that $\mathrm{Im}\phi$ is a field.

Solution. First we will show that $\mathrm{Ker}\phi = \langle p(x) \rangle$ is a maximal ideal. Suppose not. Then there is a proper ideal I such that $\mathrm{Ker}\phi \subset I$ and $\mathrm{Ker}\phi \neq I$. Since $\boldsymbol{Q}[x]$ is a principal ideal domain, there is $q(x)$ such that $I = \langle q(x) \rangle$. Since $p(x) \in \langle p(x) \rangle \subset I = \langle q(x) \rangle$, $q(x) \mid p(x)$. As $p(x)$ is irreducible $\langle p(x) \rangle = \langle q(x) \rangle$ or $q(x)$ is a nonzero constant. Neither of the cases are possible. Therefore, $\mathrm{Ker}\phi$ is maximal. By isomorphism theorem $\boldsymbol{Q}[x]/\mathrm{Ker}\phi \approx \mathrm{Im}\phi$ and the left hand side is a field as $\mathrm{Ker}\phi$ is a maximal ideal. Thus $\mathrm{Im}\phi$ is a field. ■

(c) If $\beta \in \boldsymbol{C}$ satisfies $p(\beta) = 0$, then $\boldsymbol{Q}(\alpha) \approx \boldsymbol{Q}(\beta)$.

Solution. Let $\psi : \boldsymbol{Q}[x] \to \boldsymbol{C}$ $(f(x) \mapsto f(\beta))$. Then by (a) $\mathrm{Ker}\psi = \langle p(x) \rangle$. Note that by (b) $\mathrm{Im}\phi$ and $\mathrm{Im}\psi$ are fields containing $\boldsymbol{Q}$ and α or β respectively, they are also the smallest, $\mathrm{Im}\phi = \boldsymbol{Q}(\alpha)$ and $\mathrm{Im}\psi = \boldsymbol{Q}(\beta)$. Therefore,

$$\boldsymbol{Q}(\alpha) = \mathrm{Im}\phi \approx \boldsymbol{Q}[x]/\mathrm{Ker}\phi = \boldsymbol{Q}[x]/\langle p(x) \rangle = \boldsymbol{Q}[x]/\mathrm{Ker}\psi \approx \mathrm{Im}\psi = \boldsymbol{Q}(\beta).$$

■

(d) Suppose $q(x) \in \boldsymbol{Q}[x]$ is irreducible over $\boldsymbol{Q}$ of degree m, if $\gcd(n, m) = 1$, then $q(x)$ is irreducible over $\boldsymbol{Q}(\alpha)$.

Solution. Let E be a splitting field of $q(x)$ over $\boldsymbol{Q}(\alpha)$ (as $\boldsymbol{C}$ is algebraically closed, E can be taken inside $\boldsymbol{C}$, but then we need to assume the Fundamental Theorem of Algebra). Let $\beta \in E$ such that $q(\beta) = 0$. Then $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = n$ and $[\boldsymbol{Q}(\beta) : \boldsymbol{Q}] = m$. Since the minimal polynomial $q_1(x)$ of β over $\boldsymbol{Q}(\alpha)$ divides $q(x)$, $\deg q_1(x) \leq m$. Thus $[\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}] = [\boldsymbol{Q}(\alpha)(\beta) : \boldsymbol{Q}(\alpha)][\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = \deg q_1(x) \cdot n \leq nm$. Moreover, $[\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}] = [\boldsymbol{Q}(\beta)(\alpha) : \boldsymbol{Q}(\alpha)][\boldsymbol{Q}(\beta) : \boldsymbol{Q}] = [\boldsymbol{Q}(\beta)(\alpha) : \boldsymbol{Q}(\alpha)] \cdot m$. Hence $[\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}]$ is at most $m \cdot n$ and divisible by m and n. Since $\gcd(m, n) = 1$, it must be $m \cdot n$. Therefore $[\boldsymbol{Q}(\alpha)(\beta) : \boldsymbol{Q}(\alpha)] = \deg q_1(x) = m = \deg q(x)$ and $q_1(x)$ divides $q(x)$. Hence $q(x)$ is a constant multiple of $q_1(x)$ and irreducible over $\boldsymbol{Q}(\alpha)$. ■

Hiroshi Suzki @ International Christian University