November 18, 2015

Algebra II Final 2015

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

$$\langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

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 non-zero 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 R be a commutative ring with unity 1. (25pts)

   (a) Write the condition that R becomes an integral domain, and the definition of prime ideals.

   (b) Show that R is an integral domain if and only if $\{0\}$ is a prime ideal.

   (c) Let R be an integral domain. Show that for $a, b \in R$, $\langle a \rangle = \langle b \rangle$ if and only if there is a unit $u \in U(R)$ such that $b = ua$.

   (d) Let R be an integral domain and p a non-zero element such that $\langle p \rangle$ is a prime ideal. Show that p is irreducible.

   (e) Suppose R is a principal ideal domain and P is a non-zero prime ideal. Show that P is a maximal ideal.

[1] the leading coefficient is 1

2. Let R be a finite commutative ring with unity 1. (25pts)

   (a) Show that every non-zero element of R is either a zero divisor or a unit.

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

   (c) If R is an integral domain, Then the set $S = \{n \in \boldsymbol{N} \mid n \cdot 1 = 0\}$ is not empty and $p = \min S$ is a prime number.

   (d) Suppose $R = \{c_0 + c_1\alpha + c_2\alpha^2 \mid c_0, c_1, c_2 \in \boldsymbol{Z}_2\}$, a commutative ring containing $\boldsymbol{Z}_2$, and $\alpha^3 + \alpha + 1 = 0$. Write a multiplication table (with respect to multiplication).

   (e) Let R be as in (d). show that (i) R is a field and that (ii) $\beta^8 = \beta$ for all $\beta \in R$.

3. Let R be an integral domain, $R[x]$ and $R[x, y]$ rings of polynomials over R. (25pts)

   (a) Show that $U(R[x, y]) = U(R)$.

   (b) Let $f(x, y), g(x, y) \in R[x, y]$. Show that if $\langle f(x, y)\rangle = \langle g(x, y)\rangle$, then there exists $a \in U(R)$ such that $f(x, y) = a \cdot g(x, y)$.

   (c) Show that $R[x, y]$ is not a principal ideal domain.

   (d) $A = \{f(x) \in R[x] \mid f(0) = 0\}$ is a prime ideal.

   (e) A in (d) is a maximal ideal if and only if R is a field.

4. Let $a \in \boldsymbol{C}$ be a zero of a nonzero polynomial $p(x)$ in $\boldsymbol{Q}[x]$. Let $\psi : \boldsymbol{Q}[x] \to \boldsymbol{C}$ $(f(x) \mapsto f(a))$. Show the following. (25pts)

   (a) $\mathrm{Im}(\psi)$ a subring of $\boldsymbol{C}$ and $\mathrm{Ker}(\psi)$ is an ideal of $\boldsymbol{Q}[x]$.

   (b) If $\mathrm{Ker}(\psi) = \langle p(x)\rangle$, then $p(x)$ is irreducible over $\boldsymbol{Q}$ and $\mathrm{Im}(\psi)$ is a field.

   For (c), (d), (e), suppose $p(x) = x^7 + 7x + 14$, $\gamma \in \boldsymbol{R}$ is a zero of $p(x)$, and $E = \boldsymbol{Q}(\gamma)$.

   (c) Show that $[E : \boldsymbol{Q}] = 7$.

   (d) Let F be a subfield of E containing $\boldsymbol{Q}$. Then $F = \boldsymbol{Q}$ or $F = E$.

   (e) E is not the splitting field of $p(x)$ contained in $\boldsymbol{C}$.

November 18, 2015

Solutions to Algebra II Final 2015

1. Let R be a commutative ring with unity 1. (25pts)

   (a) Write the condition that R becomes an integral domain, and the definition of prime ideals.

   Solution. R is an integral domain if R does not have a zero divisor, i.e., if $ab = 0$ implies $a = 0$ or $b = 0$ for $a, b \in R$. A nonempty subset A of R is a prime ideal if (i) A is a proper ideal, i.e., $A \neq R$ and for all $a, b \in A$ and $r \in R$, $a - b \in A$ and $ra \in A$, and if (ii) for $a, b \in R$, $ab \in A$ implies $a \in A$ or $b \in A$.

   (b) Show that R is an integral domain if and only if $\{0\}$ is a prime ideal.

   Solution. First note that $0 \neq 1 \in R$, $\{0\}$ is a proper ideal. Suppose R is an integral domain and $ab \in \{0\}$ for $a, b \in R$. Then $ab = 0$ and $a = 0$ or $b = 0$. Thus $a \in \{0\}$ or $b \in \{0\}$ and $\{0\}$ is a prime ideal.

   Next assume that $\{0\}$ is a prime ideal. If $ab = 0$ for some $a, b \in R$. Then $ab \in \{0\}$. Since $\{0\}$ is a prime ideal, $a \in \{0\}$ or $b \in \{0\}$, i.e., $a = 0$ or $b = 0$.

   (c) Let R be an integral domain. Show that for $a, b \in R$, $\langle a \rangle = \langle b \rangle$ if and only if there is a unit $u \in U(R)$ such that $b = ua$.

   Solution. Suppose $b = ua$ for some unit u. Then $a = u^{-1}b$. Hence $b = ua \in \langle a \rangle$ and $\langle b \rangle \subseteq \langle a \rangle$. Moreover, $a = u^{-1}b \in \langle b \rangle$ and $\langle a \rangle \subseteq \langle b \rangle$. Hence $\langle a \rangle = \langle b \rangle$. Conversely assume that $\langle a \rangle = \langle b \rangle$. Since $b \in \langle b \rangle = \langle a \rangle$, $b = ua$ for some $u \in R$. Similarly, $a \in \langle a \rangle = \langle b \rangle$, $a = vb$ for some $v \in R$. In particular, if $b = 0$, then $a = 0$, in which case $b = 0 = 1a$ and the assertion holds. Assume $b \neq 0$. Since $b = ua = uvb$, $(1 - uv)b = 0$. $1 = uv$ and $u \in U(R)$. Hence the assertion holds.

   (d) Let R be an integral domain and p a non-zero element such that $\langle p \rangle$ is a prime ideal. Show that p is irreducible.

   Solution. Since $p \neq 0$ and $\langle p \rangle \neq \langle 1 \rangle$, by (b), p is not a unit of R. Suppose $p = ab$. Then $ab \in \langle p \rangle$ and $\langle p \rangle$ is a prime ideal, $a \in \langle p \rangle$ or $b \in \langle p \rangle$. By symmetry we may assume that $a \in \langle p \rangle$. Then $a = pq = abq$ for some $q \in R$. Since $a(1 - bq) = 0$ and $a \neq 0$, $bq = 1$ and b is a unit. Thus p is irreducible.

   (e) Suppose R is a principal ideal domain and P is a non-zero prime ideal. Show that P is a maximal ideal.

   Solution. Since R is a principal ideal domain, there exists $P = \langle p \rangle$. Since $P \neq \{0\}$, $p \neq 0$. Since P is a prime ideal, p is irreducible by (d). Suppose $P \subseteq Q \subset R$, i.e., Q is a proper ideal containing P. Since R is a principal ideal domain, $Q = \langle q \rangle$ for some non-zero non-unit element $q \in Q$. Since $p \in \langle p \rangle = P \subseteq Q = \langle q \rangle$. Thus there exists $r \in R$ such that $p = rq$. Since p is irreducible and q is a non-unit element, r is a unit and by (c), $P = \langle p \rangle = \langle q \rangle = Q$ and P is a maximal ideal.

2. Let R be a finite commutative ring with unity 1. (25pts)

   (a) Show that every non-zero element of R is either a zero divisor or a unit.

   Solution. Let a be a non-zero element of R. Assume that a is not a zero-divisor. Let $\phi : R \to R$ $(x \mapsto ax)$. Then $ax = ay$ implies $a(x - y) = 0$ and we have $x = y$. Therefore, ϕ is one-to-one. Since R is a finite ring, ϕ is a bijection, and there exist $b \in R$ such that $1 = \phi(b) = ab$. Therefore, a is a unit.

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

   Solution. Let a be a non-zero element of R. Since R is an integral domain, a is not a zero divisor. Hence by (a), a is a unit. Since R is a commutative ring with unity and every non-zero element of R is a unit, R is a field.

   (c) If R is an integral domain, Then the set $S = \{n \in \boldsymbol{N} \mid n \cdot 1 = 0\}$ is not empty and $p = \min S$ is a prime number.

   Solution. Let $T = \{n \cdot 1 \mid n \in \boldsymbol{N}\}$. Since $T \subseteq R$ and R is a finite set, there are $m, n \in \boldsymbol{N}$ with $n > m$ such that $n \cdot 1 = m \cdot 1$. Hence $(n - m) \cdot 1 = 0$ with $n - m \in \boldsymbol{N}$ and $S \neq \emptyset$. Let $p = \min S$. Then p is a positive integer and $p \neq 1$ as $1 \neq 0$. Suppose p is a composite, i.e., $p = ab$ with $1 < a, b < p$. Then $0 = p \cdot 1 = ab \cdot 1 = (a \cdot 1)(b \cdot 1)$ and $a \cdot 1 = 0$ or $b \cdot 1 = 0$ as R is an integral domain. This contradicts the choice of p, which is the smallest element in S.

   (d) Suppose $R = \{c_0 + c_1\alpha + c_2\alpha^2 \mid c_0, c_1, c_2 \in \boldsymbol{Z}_2\}$, a commutative ring containing $\boldsymbol{Z}_2$, and $\alpha^3 + \alpha + 1 = 0$. Write a multiplication table (with respect to multiplication).

   Solution. Since $\alpha^3 + \alpha + 1 = 0$ and $c_0, c_1, c_2 \in \boldsymbol{Z}_2$, $\alpha^3 = 1 + \alpha$. Hence $\alpha^4 = \alpha \cdot \alpha^3 = \alpha + \alpha^2$ and $\alpha^5 = 1 + \alpha + \alpha^2$, ...

	α^i	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0		0	0	0	0	0	0	0	0
1	α^0	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
α	α^1	0	α	α^2	$\alpha+\alpha^2$	$1+\alpha$	1	$1+\alpha+\alpha^2$	$1+\alpha^2$
$1+\alpha$	α^3	0	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$	α^2	1	α
α^2	α^2	0	α^2	$1+\alpha$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	α	$1+\alpha^2$	1
$1+\alpha^2$	α^6	0	$1+\alpha^2$	1	α^2	α	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$
$\alpha+\alpha^2$	α^4	0	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	1	$1+\alpha^2$	$1+\alpha$	α	α^2
$1+\alpha+\alpha^2$	α^5	0	$1+\alpha+\alpha^2$	$1+\alpha^2$	α	1	$\alpha+\alpha^2$	α^2	$1+\alpha$

   (e) Let R be as in (d). show that (i) R is a field and that (ii) $\beta^8 = \beta$ for all $\beta \in R$.

   Solution. Since in each row of non-zero element, 1 appears, R is a field. Since $\alpha^7 = 1$ and $R\backslash\{0\}$ is generated by α multiplicatively, $\beta^7 = 1$ for every non-zero element of R. Thus $\beta^8 = \beta$ for all elements of R.

3. Let R be an integral domain, $R[x]$ and $R[x, y]$ rings of polynomials over R. (25pts)

   (a) Show that $U(R[x, y]) = U(R)$.

   Solution. Since $R[x, y] = (R[x])[y]$, by I (b), $U(R[x, y]) = U(R[x]) = U(R)$.

   (b) Let $f(x, y), g(x, y) \in R[x, y]$. Show that if $\langle f(x, y)\rangle = \langle g(x, y)\rangle$, then there exists $a \in U(R)$ such that $f(x, y) = a \cdot g(x, y)$.

   Solution. By (a) and Problem 1 (c), there exists $a \in U(R)$ such that $f(x, y) = a \cdot g(x, y)$.

   (c) Show that $R[x, y]$ is not a principal ideal domain.

   Solution. Let $\phi : R[x, y] \to R[x]$ $(f(x, y) \mapsto f(x, 0))$. Then ϕ is an onto ring homomorphism. Let $A = \mathrm{Ker}(\phi)$. Then $R[x, y]/A \approx R[x]$. Since $R[x]$

is an integral domain by I (a), A is a prime ideal. Since $y \in A$, and $1 \notin A$, A is an nonzero proper ideal. Suppose by way of contradiction, $R[x, y]$ is a principal ideal domain. Then by Problem 1 (e), A is a maximal ideal and $R[x, y]/A \approx R[x]$ is a field. This is a contradiction as $U(R[x]) = U(R)$ and x is not a unit.

(d) $A = \{f(x) \in R[x] \mid f(0) = 0\}$ is a prime ideal.

Solution. Let $\psi : R[x] \to R\,(f(x) \mapsto f(0))$, Then ψ is an onto ring homomorphism. Clearly $A = \mathrm{Ker}(\psi)$. Since $R[x]/A \approx R$ and R is an integral domain, A is a prime ideal.

(e) A in (d) is a maximal ideal if and only if R is a field.

Solution. By the isomorphism $R[x]/A \approx R$, R is a field if and only if A is a maximal ideal.

4. Let $a \in \boldsymbol{C}$ be a zero of a nonzero polynomial $p(x)$ in $\boldsymbol{Q}[x]$. Let $\psi : \boldsymbol{Q}[x] \to \boldsymbol{C}\ (f(x) \mapsto f(a))$. Show the following. (25pts)

(a) $\mathrm{Im}(\psi)$ a subring of $\boldsymbol{C}$ and $\mathrm{Ker}(\psi)$ is an ideal of $\boldsymbol{Q}[x]$.

Solution. ψ is a ring homomorphism. So if $\psi(f(x)), \psi(g(x)) \in \mathrm{Im}(\psi)$ with $f(x), g(x) \in \boldsymbol{Q}[x]$, $\psi(f(x)) - \psi(g(x)) = f(0) - g(0) = \psi(f(x) - g(x)) \in \mathrm{Im}(\psi)$. Moreover, $\psi(f(x))\psi(g(x)) = f(0)g(0) = \psi(f(x)g(x)) \in \mathrm{Im}(\psi)$. Hence $\mathrm{Im}(\psi)$ is a subring of $\boldsymbol{C}$. Suppose $f(x), g(x) \in \mathrm{Ker}(\psi)$ and $h(x) \in \boldsymbol{Q}[x]$. Then $\psi(f(x) - g(x)) = f(0) - g(0) = 0 - 0 = 0$ and $\psi(h(x)f(x)) = h(0)f(0) = h(0) \cdot 0 = 0$. Hence $\mathrm{Ker}(\psi)$ is an ideal of $\boldsymbol{Q}[x]$.

(b) If $\mathrm{Ker}(\psi) = \langle p(x) \rangle$, then $p(x)$ is irreducible over $\boldsymbol{Q}$ and $\mathrm{Im}(\psi)$ is a field.

Solution. Since $\boldsymbol{Q}[x]/\mathrm{Ker}(\psi) \approx \mathrm{Im}(\psi)$ and $\mathrm{Im}(\psi)$ is a subring of $\boldsymbol{C}$ containing 1, it is an integral domain. Hence $A = \mathrm{Ker}(\psi)$ is a prime ideal containing $p(x)$. Hence by II (a), $\boldsymbol{Q}[x]$ is a principal ideal domain and by Problem 1 (e), A is a maximal ideal. Since $\langle p(x) \rangle = A$ is a prime ideal, $p(x)$ is irreducible by Problem 1 (d) and $\boldsymbol{Q}[x]/A \approx \mathrm{Im}(\psi)$ is a field.

For (c), (d), (e), suppose $p(x) = x^7 + 7x + 14$, $\gamma \in \boldsymbol{R}$ is a zero of $p(x)$, and $E = \boldsymbol{Q}(\gamma)$.

(c) Show that $[E : \boldsymbol{Q}] = 7$.

Solution. By Eisenstein's criterion, $p(x)$ is irreducible over $\boldsymbol{Q}$. Since γ is a zero of an irreducible polynomial $p(x)$, $[E : \boldsymbol{Q}] = \deg p(x) = 7$.

(d) Let F be a subfield of E containing $\boldsymbol{Q}$. Then $F = \boldsymbol{Q}$ or $F = E$.

Solution. Since $7 = [E : \boldsymbol{Q}] = [E : F][F : \boldsymbol{Q}]$, $[E : F] = 1$ or $[F : \boldsymbol{Q}] = 1$. Hence $F = E$ or $F = \boldsymbol{Q}$.

(e) E is not the splitting field of $p(x)$ contained in $\boldsymbol{C}$.

Solution. Since $p'(x) = 7x^6 + 7 > 0$, $p(x)$ is increasing and γ is the only real zero. Hence other zeros are not real and they are not contained in $\boldsymbol{Q}(a)$ and E is not the splitting field. (The fact that $\boldsymbol{C}$ is algebraically closed is assumed.)

Hiroshi Suzuki @ International Christian University