Math 306, Spring 2012
Midterm 1 Review Solutions

(1) (a) Let R be an integral domain. Prove that the set $U(R)$ of units of R is an abelian multiplicative group.
(b) Prove that, if K is a field, then $K[x, y]$ is not a principal ideal domain.

Solution:
(a) Since $1 \in U(R)$, we know that $U(R)$ is nonempty and contains an identity element. Associativity and commutativity are inherited from R. If $u \in U(R)$, then there is $u' \in R$ such that $uu' = 1$. Therefore u' is a unit as well, so $u' \in U(R)$. Let $u, v \in U(R)$. Then there are $u', v' \in R$ such that $uu' = 1 = vv'$. Then $(uv)(u'v') = 1$, so uv is a unit. Hence $U(R)$ is closed under multiplication. Therefore $U(R)$ is an abelian group.
(b) Consider the ideal $I = (x, y)$. Suppose that I is principal, so $I = (d)$ for some $d \in K[x, y]$. Therefore $d|x$ and $d|y$, so d must be a unit, since x and y are coprime. Therefore $I = K[x, y]$. In particular we have $1 \in I$. Every element in I is of the form $px + qy$, where $p, q \in K[x, y]$. So $1 = px + qy$ for some $p, q \in K[x, y]$. However, every element of the form $px + qy$ has no nontrivial constant term, a contradiction. So I is not principal, and $K[x, y]$ is not a principal ideal domain.

(2) Let R be a ring and let x and y be indeterminates. Recall that $R[x, y]$ can be thought of as $(R[x])[y]$. It is easy to see that $R[x, y] \cong R[y, x]$. By induction we can define $R[x_1, \ldots, x_n]$ where the x_i are all indeterminates. Let $p = 2x^2y - 3xy^3z + 4y^2z^5$ and $q = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$ be elements in $\mathbb{Z}[x, y, z]$.
(a) Write p and q as polynomials in x with coefficients in $\mathbb{Z}[y, z]$. Find the degrees of p and q.
(b) Write p and q as polynomials in y with coefficients in $\mathbb{Z}[x, z]$. Find the degrees of p and q.

Solution:
(a) We can write $p = 4y^2z^5 - (3y^3z)x + (2y)x^2$ which has degree 2 and $q = (7 + 5y^3z^4 - 3z^3)x^2$ which has degree 2.
(b) We can write $p = (2x^2)y + (4z^5)y^2 - (3xz)y^3$ which has degree 3 and $q = (7x^2 - 3x^2z^3) + (5x^2z^4)y^3$ which has degree 3.

(3) Prove that $\mathbb{Q}[x, y]$ is not a PID.

Solution: Consider $I = (x, y)$. If I is principal, i.e. $I = (d)$, then $d|x$ and $d|y$. Since both x and y are irreducible and coprime, it follows that d must be a unit, so $I = \mathbb{Q}[x, y]$. However, the polynomial 1 does not lie in (x, y). If it did, then there are p and q in $\mathbb{Q}[x, y]$ such that $1 = px + qy$. However, both px and qy have zero constant term, so the sum has zero constant term, a contradiction.

(4) Find the quotient and the remainder upon division of x^3 by $x^2 + x + 1$ in $\mathbb{Z}_2[x]$.

Solution: Quotient is $x + 1$ and the remainder is 1.

(5) (a) Prove that $x^4 + 4x^3 + 6x^2 + 2x + 1$ is irreducible in $\mathbb{Q}[x]$.
(b) Find all the complex roots of $f = x^4 + 3$. Find the smallest field L containing $\mathbb{Q}$ such that f completely factors into linear polynomials in $L[x]$. (Hint: the required L will satisfy $[L\colon \mathbb{Q}] = 8$.)

Solution:
(a) Let $f = x^4 + 4x^3 + 6x^2 + 2x + 1$. Then $f(x + 1) = x^4 + 8x^3 + 24x^2 + 30x + 14$, which is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion and $p = 2$. Hence f is irreducible in $\mathbb{Q}[x]$ as well.
(b) The roots of f are given by $\alpha_1 = \sqrt[4]{3}\, e^{\pi i/4}$, $\alpha_2 = \sqrt[4]{3}\, e^{3\pi i/4}$, $\alpha_3 = \sqrt[4]{3}\, e^{5\pi i/4}$, $\alpha_4 = \sqrt[4]{3}\, e^{7\pi i/4}$. So we are interested in computing $[\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\colon \mathbb{Q}]$. Now each of the α_i can be written as $\sqrt[4]{3}\left(\frac{\pm 1 \pm i}{\sqrt{2}}\right)$. So $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}(\sqrt[4]{3}\sqrt{2}(1+i), \sqrt[4]{3}\sqrt{2}(1-i))$. Call this field L. We will prove that $L = \mathbb{Q}(\sqrt[4]{3}\sqrt{2}, i)$. Clearly $L \subseteq \mathbb{Q}(\sqrt[4]{3}\sqrt{2}, i)$. Conversely, it is easy to see that $\sqrt[4]{3}\sqrt{2}(1 + i) + \sqrt[4]{3}\sqrt{2}(1 - i)$ lies in L, so $\sqrt[4]{3}\sqrt{2}$ lies in L. Also, we know that $2\sqrt[4]{3}\sqrt{2}\, i = \sqrt[4]{3}\sqrt{2}(1 + i) - \sqrt[4]{3}\sqrt{2}(1 - i)$ lies in L, so i also lies in L. Therefore $\mathbb{Q}(\sqrt[4]{3}\sqrt{2}, i) \subseteq L$, as required. By the tower law, we know that $[L\colon \mathbb{Q}] = 8$.

(6) (a) Let $n \in \mathbb{Z}_{\geq 2}$ and suppose that $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ has a factor $ax + b$. Show $a|a_n$ and $b|a_0$.
(b) Suppose α is a rational root of a monic polynomial in $\mathbb{Z}[x]$. Prove that α is an integer.

Solution:

(a) Suppose that $a_n x^n + \cdots + a_1 x + a_0 = (ax+b)(c_{n-1}x^{n-1} + \cdots c_1 x + c_0)$. Then $ac_{n-1} = a_n$ and $bc_0 = a_0$. Therefore $a|a_n$ and $b|a_0$.

(b) Let $\alpha = p/q$ be a rational root of the polynomial $x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$. We may assume that p and q are coprime. Then $(p/q)^n + b_{n-1}(p/q)^{n-1} + \cdots + b_1(p/q) + b_0 = 0$ in $\mathbb{Q}$. Multiply the whole expression by q^n to get $p^n + b_{n-1}pq + \cdots + b_1 pq^{n-1} + b_0 q^n = 0$. Therefore q must divide p^n. But q and p are coprime, so q must equal 1. Therefore α is an integer.

(7) Describe the subfields of $\mathbb{C}$ of the form $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ and $\mathbb{Q}(e^2+1)$. Write the first in the form $\mathbb{Q}[x]/(m)$ where m is an irreducible polynomial.

Solution: We have that $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \{p + q\sqrt{5} + \sqrt{7} + r\sqrt{35} \colon p, q, r \in \mathbb{Q}\}$. We also know that $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \cong \mathbb{Q}(\sqrt{5} + \sqrt{7})$ and since the minimal polynomial for $\sqrt{5} + \sqrt{7}$ is $x^4 - 24x^2 + 4$ (see problem 4(b) on homework 3), $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ is isomorphic to $Q[x]/(x^4 - 24x^2 + 4)$.

For the second field, $\mathbb{Q}(e^2+1) \cong \mathbb{Q}(e^2) \cong \{p_1 + p_2 e^2 + p_3 e^4 + p_4 e^6 + \cdots \colon p_i \in \mathbb{Q}\}$.

(8) Let $\mathbb{A}$ be the collection of all $\alpha \in \mathbb{C}$ such that α is algebraic over $\mathbb{Q}$.

(a) Prove that, if $\alpha \in \mathbb{A}^*$, then $\alpha^{-1} \in \mathbb{A}$.

(b) Prove that, if $\alpha, \beta \in \mathbb{A}$, then $\alpha - \beta$ and $\alpha\beta$ belong to $\mathbb{A}$.

(c) Conclude that $\mathbb{A}$ is a field.

(Hint: Recall that, if $K(\alpha) \colon K$ is finite, then α is algebraic over K.)

Solution:

(a) Let α be nonzero. If α is algebraic over $\mathbb{Q}$, then $[\mathbb{Q}(\alpha) \colon \mathbb{Q}]$ is finite. Since $1/\alpha$ belongs to $\mathbb{Q}(\alpha)$, it follows by the tower law that $[\mathbb{Q}(1/\alpha) \colon \mathbb{Q}]$ is also finite, since it divides $[\mathbb{Q}(\alpha) \colon \mathbb{Q}]$. Hence $1/a$ belongs to $\mathbb{A}$.

(b) If α and β belong to $\mathbb{A}$, then $[\mathbb{Q}(\alpha, \beta) \colon \mathbb{Q}]$ is finite. Since $\alpha - \beta$ and $\alpha\beta$ belong to $\mathbb{Q}(\alpha, \beta)$, it follows from the tower law that $[\mathbb{Q}(\alpha - \beta) \colon \mathbb{Q}]$ and $[\mathbb{Q}(\alpha\beta) \colon \mathbb{Q}]$ both divide $[\mathbb{Q}(\alpha, \beta) \colon \mathbb{Q}]$, and hence are finite. Therefore $\alpha - \beta$ and $\alpha\beta$ both belong to $\mathbb{A}$.

(c) Since $\mathbb{A}$ is closed under subtraction, multiplication and inverses, then it must be a field.

(9) Let K be a field and let x be an indeterminate. Denote by $K(x)$ the field of fractions of $K[x]$. Let $t = p/q \in K(x)$, where p and q are coprime polynomials in $K[x]$ and $q \neq 0$.

(a) Is $K(x)$ an extension of $K(t)$, or is $K(t)$ an extension of $K(x)$? Explain.

(b) Prove that $f = p - tq \in K(t)[x]$ is irreducible over $K(t)$.

(c) Prove that $[K(x) \colon K(t)] = \max\{\deg p, \deg q\}$.

Solution:

(a) Here $K(x)$ is an extension of $K(t)$ because $t \in K(x)$, so $K(t) \subseteq K(x)$.

(b) Clearly f is a linear polynomial in $(K[x])[t]$ so it is irreducible in that ring. But $(K[x])[t] \cong K[t, x] \cong (K[t])[x]$, so f is irreducible in $(K[t])[x]$. By Gauss's Lemma, we conclude that f is irreducible in $K(t)[x]$.

(c) Clearly f is an irreducible polynomial in $K(t)[x]$ with x as a root, so $[K(x) \colon K(t)]$ is equal to the degree of f, which is $\max\{\deg p, \deg q\}$.

(10) Determine, with explanation, whether the following are true or false.

(a) Every field has a nontrivial extension.

(b) Every field has a nontrivial algebraic extension.

(c) Every simple extension is algebraic.

(d) Every root of unity is algebraic over $\mathbb{Q}$

Solution:

(a) True, adjoining a variable gives a nontrivial extension.

(b) False, take $\mathbb{A}$ from problem 8 above. This has no algebraic extension in $\mathbb{C}$,

(c) False, take $\mathbb{Q}(\tau)$ where τ is transcendental.

(d) True, roots of unity are by definition the zeros of $x^n - 1$ for some n.