# Mathematics 351 – Abstract Algebra I
## Solutions for Midterm Exam 1 – October 1, 2007

I. *Terminology.*

A) (5) Give an example of a ring $R$ that is *not* a *commutative ring.*

*Solution:* The ring of $2 \times 2$ matrices with real entries, $M_{2\times 2}(\mathbf{R})$, is one example.

B) (5) What does it mean to say that $R$ is a *ring with identity*?

*Solution:* $R$ is a ring with identity if there is a *multiplicative identity* in $R$: an element $1_R$ satisfying $1_R \cdot a = a \cdot 1_R = a$ for all $a \in R$.

C) (5) What does it mean to say that $u \in R$ is a *unit*?

*Solution:* $u$ is a unit if $u$ has a multiplicative inverse in $R$ (an element $x$ such that $u \cdot x = 1_R = x \cdot u$. Note that this only makes sense if $R$ is a ring with identity(!)

D) (5) Is every commutative ring with identity an *integral domain*? If so, say why. If not, give a counterexample.

*Solution:* The answer is *no*. The ring $\mathbf{Z}_6$ is a commutative ring with identity, but it is not an integral domain, since for instance, $[2][3] = 0$, but $[2] \neq [0]$ and $[3] \neq [0]$.

II. Let $R$ be a ring. Let $b$ be any one particular element of $R$, and let

$$C_b = \{a \in R : a \cdot b = b \cdot a\}.$$

A) (10) Show that $C_b$ is a subring of $R$.

*Solution:* We use the criterion from Theorem 3.6 in Hungerford. First notice that $C_b$ is not empty, since $0_R \cdot b = b \cdot 0_R = 0_R$. Hence $0_R \in C_b$. Let $a, a' \in C_b$. Then by the distributive law

$$(a - a') \cdot b = a \cdot b - a' \cdot b = b \cdot a - b \cdot a' = b \cdot (a - a').$$

This shows $a - a' \in C_b$ so $C_b$ is closed under differences. Similarly by associativity of multiplication,

$$(a \cdot a') \cdot b = a \cdot (a' \cdot b) = a \cdot (b \cdot a') = (a \cdot b) \cdot a' = (b \cdot a) \cdot a' = b \cdot (a \cdot a').$$

Hence $C_b$ is also closed under products, and hence is a subring of $R$.

B) (10) Let $S$ be a second ring, and let $\varphi : R \to S$ be a ring homomorphism. Show that if $b \in R$, then $\varphi(C_b) \subseteq C_{\varphi(b)} \subseteq S$.

*Solution:* Let $a \in C_b$, so $a \cdot b = b \cdot a$. By the definition of a ring homomorphism,

$$\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b) = \varphi(b \cdot a) = \varphi(b) \cdot \varphi(a).$$

This shows $\varphi(a) \in C_{\varphi(b)}$. Hence $\varphi(C_b) \subset C_{\varphi(b)}$.

III. Let $F[x]$ be the ring of polynomials with coefficients in a field $F$.

A) (10) Show that the quotient and remainder under the division of $f(x)$ by $g(x)$ in $F[x]$ are unique.

*Solution:* Suppose $f(x) = q(x)g(x) + r(x)$ and $f(x) = q_1(x)g(x) + r_1(x)$, where both $r(x)$ and $r_1(x)$ are either zero or have degree less than the degree of $g(x)$. Then subtracting these equations shows $0 = (q(x) - q_1(x))g(x) + r(x) - r_1(x)$, so $r(x) - r_1(x) = (q_1(x) - q(x))g(x)$. If $r(x) - r_1(x) \neq 0$, then it is a polynomial of degree $\leq \deg(g)$. However, $\deg((q_1(x)-q(x))g(x)) = \deg(q_1(x)-q(x)) + \deg(g(x)) \geq \deg(g(x))$. This gives a contradiction, so $r(x) = r_1(x)$ and $q(x) = q_1(x)$.

B) (5) *Define:* $f(x)$ is *irreducible* in $F[x]$.

*Solution:* $f(x)$ is irreducible if in every factorization $f(x) = g(x)h(x)$ in $F[x]$, one of $g(x), h(x)$ is a unit (a nonzero constant polynomial), and the other is an associate of $f(x)$.

C) (10) In what sense are factorizations of polynomials into irreducibles unique? (State the theorem that answers this question; you do not need to prove it.)

*Solution:* The sense in which irreducible factorizations are unique in $F[x]$ is that if

$$f(x) = p_1(x) \cdots p_s(x) \qquad \text{and} \qquad q_1(x) \cdots q_s(x),$$

where all the $p_i(x)$ and $q_j(x)$ are irreducible in $F[x]$, then $r = s$, and for each $1 \leq i \leq s$, there exists some $j$ such that $p_i(x)$ and $q_j(x)$ are associates.

IV.

A) (10) Let $F$ be a field. Show that $a \in F$ is a root of $f(x) \in F[x]$ if and only if $(x-a)|f(x)$ in $F[x]$.

*Solution:* Use the division algorithm in $F[x]$, dividing $x - a$ into $f(x)$ to write $f(x) = q(x)(x-a) + r(x)$, where either $r$ is zero, or else $\deg(r) < \deg(x-a) = 1$. If $a \in F$ is a root of $f(x)$, then $0 = f(a) = q(a)(a-a) + r$, so $r = 0$. This shows $(x-a)|f(x)$. Conversely, if $(x-a)|f(x)$, then $r = 0$, so $f(a) = q(a)(a-a) = 0$, so $a$ is a root of $f(x)$.

B) (10) Let $F$ be a field. If $a_1, \ldots, a_n$ are *distinct* roots of $f(x) \in F[x]$ in $F$, show that $((x-a_1)(x-a_2)\cdots(x-a_n))\,|f(x)$. (Hint: induction on $n$).

*Solution:* Following the hint, part A is the base case for the induction. So assume that whenever a polynomial $g(x)$ in $F[x]$ has $k$ distinct roots $a_1, \ldots, a_k$, then $((x - a_1) \cdot \cdots \cdot (x - a_k)) | g(x)$. Assume now that $f(x)$ is a polynomial with $k + 1$ distinct roots in $F$, say $a_1, \ldots, a_{k+1}$. By part A, we know that $(x - a_{k+1}) | f(x)$ so write

$$f(x) = ((x - a_1) \cdot \cdots \cdot (x - a_k))q(x) \tag{1}$$

for some $q(x) \in F[x]$. If we substitute $x = a_i$, for any $i$, $1 \leq i \leq k$, then $0 = f(a_i) = (a_i - a_{k+1})q(a_i)$. The first factor cannot be zero since the $a_j$'s are distinct. Hence $q(x)$ must have $a_1, \ldots, a_k$ as roots, and by induction $((x - a_1) \cdot \cdots \cdot (x - a_k)) | q(x)$. This means

$$q(x) = ((x - a_1) \cdot \cdots \cdot (x - a_k))s(x) \tag{2}$$

for some $s(x) \in F[x]$. Hence combining (1) and (2),

$$f(x) = (x - a_{k+1})((x - a_1) \cdot \cdots \cdot (x - a_k))s(x)$$

which shows what we wanted to prove.

C) (5) What are the roots of $x^2 + 2x \in \mathbf{Z}_8[x]$ in $\mathbf{Z}_8$? Why is your result *not a contradiction* to part B?

*Solution:* $x = 0, 2, 4, 6$ all satisfy $x^2 + 2x = 0$ in $\mathbf{Z}_8$. This is not a contradiction to part B since $\mathbf{Z}_8$ is *not a field.* The statement in part B does not apply.

V. All parts of this question refer to

$$f(x) = 5x^5 - 12x^3 + 36x^2 + 18 \in \mathbf{Q}[x].$$

A) (5) List all rational numbers that could be roots of $f$ according to the Rational Root Test.

*Solution:* The possible rational roots of $f(x)$ are all rational numbers in lowest terms of the form $p/q$, where $p|18$ and $q|5$, so:

$$x = \pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18, \pm\frac{1}{5}, \pm\frac{2}{5}, \pm\frac{3}{5}, \pm\frac{6}{5}, \pm\frac{12}{5}, \pm\frac{18}{5}.$$

B) (5) Use any applicable method to decide whether $f$ is irreducible in $\mathbf{Q}[x]$, and state which criterion or criteria you are using.

*Solution:* By the Eisenstein Criterion with $p = 2$, $f(x)$ is irreducible in $\mathbf{Q}[x]$: $2 \not| 5$, $2|(-12), 2|36, 2|18$, but $2^2 = 4 \not| 18$.