Math 302 **Modern Algebra** **Spring 2009**

Exam 2 Solutions

1. (36 points) Let S be the set of integers with an addition $\oplus$ and multiplication $\odot$ defined for all $a, b \in S$ by

$$a \oplus b = a + b - 1 \qquad \text{and} \qquad a \odot b = a + b - ab.$$

(The $+$, $-$, and $\cdot$ symbols denote ordinary integer addition, subtraction, and multiplication, respectively.) It can be shown that S is a commutative ring with $0_S = 1$ under these operations.

(a) Verify ring axiom R10 Existence of a Multiplicative Identity for S.

Proof: We need to show there exists an element $1_S \in S$ such that for all $a \in S$,

$$a \odot 1_S = a \qquad \text{and} \qquad 1_S \odot a = a.$$

Find a 1_S.
The element 1_S must satisfy

$$a \odot 1_S = a$$

for all $a \in S$. This means

$$a + 1_S - a1_S = a$$
$$1_S(1 - a) = 0$$

This implies

$$1_S = 0 \qquad \text{or} \qquad a = 1.$$

Since this must hold for all integers a, not just $a = 1$, then $1_S = 0$. Choose $1_S = 0$.

Verify that 1_S satisfies:
(i) Domain: $1_S \in S$
(ii) Propositional Function:
$(\forall a \in S)\,[a \odot 1_S = a \wedge 1_S \odot a = a]$

Since $1_S = 0$ is an integer, then $1_S \in S$. To prove (ii), suppose a is an arbitrary integer. We need to show

$$a \odot 1_S = a \qquad \text{and} \qquad 1_S \odot a = a.$$

We have

$$a \odot 1_S = a \odot 0 = a + 0 + a0 = a$$
$$1_S \odot a = 0 \odot a = 0 + a + 0a = a$$

as required.

Thus $1_S = 0$ is a multiplicative identity for S.

(b) Verify ring axiom R11 Zero Factor Property for S.

We need to show

$$(\forall a \in S)\,(\forall b \in S)\,[a \odot b = 0_S \to a = 0_S \vee b = 0_S].$$

Proof: Suppose a and b are arbitrary integers in S. Suppose

$$a \odot b = 0_S = 1.$$

We need to show that

$$a = 0_S = 1 \qquad \text{or} \qquad b = 0_S = 1.$$

By the hypothesis,

$$a \odot b = a + b - ab = 1$$
$$a - 1 + b - ab = 0$$
$$(a - 1) - b(a - 1) = 0$$
$$(a - 1)(1 - b) = 0$$

Therefore

$$a = 1 = 0_S \qquad \text{or} \qquad b = 1 = 0_S,$$

as required. Thus S satisfies the Zero Factor Property.

1. (continued)

(c) Let R be the set of integers with the ordinary integer addition $+$ and multiplication $\cdot$. Define a function $f : R \to S$ by

$$f(r) = 1 - r \qquad \text{for each } r \in R.$$

Show that f is a ring homomorphism.

We need to verify the two properties of a ring homomorphism.

RH1. Preservation of Addition. For all $a, b \in S$, $f(a + b) = f(a) \oplus f(b)$.
Proof: Suppose a and b are arbitrary integers in R. We need to show

$$f(a + b) = f(a) \oplus f(b).$$

We have

$$\begin{aligned} f(a + b) &= 1 - (a + b) \\ f(a) \oplus f(b) &= (1 - a) \oplus (1 - b) = (1 - a) + (1 - b) - 1 = 1 - a - b \end{aligned}$$

Then $f(a + b) = f(a) \oplus f(b)$, as required. Therefore f preserves addition.

RH2. Preservation of Multiplication. For all $a, b \in S$, $f(a \cdot b) = f(a) \odot f(b)$.
Proof: Suppose a and b are arbitrary integers in R. We need to show

$$f(a \cdot b) = f(a) \odot f(b).$$

We have

$$\begin{aligned} f(a \cdot b) &= 1 - (ab) \\ f(a) \odot f(b) &= (1 - a) \odot (1 - b) = (1 - a) + (1 - b) - (1 - a)(1 - b) \\ &= 2 - a - b - (1 - a - b + ab) = 1 - ab \end{aligned}$$

Then $f(a \cdot b) = f(a) \odot f(b)$, as required. Therefore f preserves multiplication.

Thus f is a ring homomorphism.

2. (24 points) Let R be a ring.

(a) Prove Theorem 3.3: For each element a in a ring R, the equation $a+x = 0_R$ has a unique solution. What does this imply about additive inverses in a ring?

Proof: Suppose a is an arbitrary element in R. We need to show that the equation $a + x = 0_R$ has a unique solution. By axiom R5f, there exists a solution to this equation. So we only need to show the solution is unique.

Suppose $b, c \in R$ are both solutions to the equation $a + x = 0_R$. Then

$$a + b = 0_R \qquad \text{and} \qquad a + c = 0_R.$$

We need to show $b = c$. We have

$$\begin{aligned} b &= b + 0_R && \text{(by R4, the property of the additive identity)} \\ &= b + (a + c) && \text{(since } a + c = 0_R\text{)} \\ &= (b + a) + c && \text{(by R2 Associative Law of Addition)} \\ &= (a + b) + c && \text{(by R3 Commutative Law of Addition)} \\ &= 0_R + c && \text{(since } a + b = 0_R\text{)} \\ &= c && \text{(by R4, the property of the additive identity)} \end{aligned}$$

Therefore $b = c$, as required.

Since the additive inverse of a is the solution to this equation, then this shows that the additive inverse of a is unique.

(b) Prove Theorem 3.5(7): Let R be a ring. If R has a multiplicative identity 1_R, then for each $a \in R$, $(-1_R)a = -a$. Justify the steps in your proof.

Proof: Suppose R has a multiplicative identity 1_R. Suppose a is an arbitrary element of R. We need to show

$$(-1_R) \cdot a = -a.$$

By part (a), the additive inverse $-a$ of a is unique. So, if we can show that $(-1_R)a$ behaves like the additive inverse, it must then follow that $(-1_R)a$ is the additive inverse, that is, $(-1_R)a = -a$. So we want to show

$$a + (-1_R)a = 0_R.$$

Consider

$$\begin{aligned} a + (-1_R) \cdot a &= 1_R \cdot a + (-1_R) \cdot a && \text{(by R10, the property of the multiplicative identity)} \\ &= [1_R + (-1_R)] \cdot a && \text{(by R8 Distributive Law)} \\ &= 0 \cdot a && \text{(by R5, the property of the additive inverse)} \\ &= 0 && \text{(by part (1) of Theorem 3.5)} \end{aligned}$$

This implies $(-1_R) \cdot a$ has the property of an additive inverse of a. Thus $(-1_R) \cdot a = -a$.

3. (12 points) Let R be a ring. Prove: For all $r \in R$, if r is a zero divisor, then r is <u>not</u> a unit.

This has symbolic form

$$(\forall r \in R)\,[r \text{ is a zero divisor} \to r \text{ is not a unit}]$$

Proof: Use a proof by contradiction. Suppose the negation

$$(\exists r \in R)\,[r \text{ is a zero divisor} \wedge r \text{ is a unit}].$$

That is, suppose there exists an element $r \in R$ such that

$$r \text{ is a zero divisor} \qquad \text{but} \qquad r \text{ is a unit.}$$

We then need to derive a contradiction.

Since r is a zero divisor, then $r \neq 0_R$ and there exists an element $s \in R$, $s \neq 0_R$ such that

$$rs = 0_R \qquad \text{or} \qquad sr = 0_R.$$

Since r is a unit, then there exists an element $r^{-1} \in R$ such that

$$rr^{-1} = 1_R \qquad \text{and} \qquad r^{-1}r = 1_R.$$

Consider the two cases:

Case 1. Suppose $rs = 0_R$. Multiplying both sides by r^{-1} on the left, we obtain

$$\begin{aligned} r^{-1}(rs) &= r^{-1}0_R \\ (r^{-1}r)s &= 0_R && \text{(by R7 Associativity of Multiplication and Theorem 3.5(i))} \\ 1_R s &= 0_R && \text{(since } r^{-1}r = 1_R\text{)} \\ s &= 0_R && \text{(by the property of the multiplicative identity)} \end{aligned}$$

This is a contradiction since $s \neq 0_R$ by assumption.

Case 2. Suppose $sr = 0_R$. Multiplying both sides by r^{-1} on the right, we obtain

$$\begin{aligned} (sr)r^{-1} &= 0_R r^{-1} \\ s(rr^{-1}) &= 0_R && \text{(by R7 Associativity of Multiplication and Theorem 3.5(i))} \\ s1_R &= 0_R && \text{(since } r^{-1}r = 1_R\text{)} \\ s &= 0_R && \text{(by the property of the multiplicative identity)} \end{aligned}$$

This is again a contradiction since $s \neq 0_R$ by assumption.

In both cases, we've derived a contradiction, which proves the result.

4. (20 points)

(a) Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree 3. Prove: If $f(x)$ has no roots in F, then $f(x)$ is irreducible. (This is part of Corollary 4.18. You should not use that corollary in your proof.)

Proof: Use a proof by contrapositive. Suppose $f(x)$ is reducible in $F[x]$. We need to show $f(x)$ has at least onoe root in F.

Since $f(x)$ is reducible in $F[x]$, then Theorem 4.10 implies that $f(x)$ can be written as the product of two polynomials of lower degree. That is, there exist polynomials $g(x), h(x) \in F[x]$ such that

$$f(x) = g(x)h(x).$$

By Theorem 4.2,

$$\deg f(x) = \deg g(x) + \deg h(x).$$

Since $\deg f(x)$ equals 3, and $\deg g(x)$ and $\deg h(x)$ are both less than $\deg f(x)$, then one of these factors must have degree 1. Suppose without loss of generality $\deg g(x) = 1$. Then

$$g(x) = cx + d \qquad \text{for some } c, d \in F,\ c \neq 0_F.$$

Since F is a field and $c \neq 0_F$, then c^{-1} exists in F and we can write

$$g(x) = c(x - dc^{-1}).$$

It then follows that $dc^{-1} \in F$ is a root of $g(x)$, so must be a root of $f(x)$ in F. This proves the result.

(b) Give an example to show that the result of part (a) does not hold for polynomials of degree 4.

Let $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ in $\mathbb{Q}[x]$. All roots of $f(x)$ are irrational so $f(x)$ has no roots in $\mathbb{Q}$. However, $f(x)$ is not irreducible since it can be written as the product of two polynomials of lower degree.

5. (16 points) Factor the polynomial $f(x) = x^4 - 6x^2 + 8$ as a product of irreducible polynomials in each of the following polynomial rings. Indicate why each factor is in fact irreducible.

(a) $\mathbb{Q}[x]$

This polynomial factors in $\mathbb{Q}[x]$ as

$$f(x) = x^4 + x^2 - 6x^2 + 8 = (x^2 - 4)(x^2 - 2) = (x - 2)(x + 2)(x^2 - 2).$$

The two factors $x - 2$ and $x + 2$ are irreducible in $\mathbb{Q}[x]$ because they have degree 1. The only roots of the factor $x^2 - 2$ are irrational so this factor has no roots in $\mathbb{Q}$. Since $x^2 - 2$ has degree 2, it follows by Corollary 4.18 that $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$.

(b) $\mathbb{Z}_7[x]$

In $\mathbb{Z}_7[x]$, the polynomial factors as

$$f(x) = (x^2 - 4)(x^2 - 2) = (x - 2)(x + 2)(x^2 - 2).$$

Note, however, that both 3 and 4 are roots of $x^2 - 2$ since

$$3^2 - 2 = 7 = 0 \qquad \text{and} \qquad 4^2 - 2 = 14 = 0.$$

Therefore $x^2 - 2 = (x - 3)(x - 4)$ and so $f(x)$ factors as

$$f(x) = (x - 2)(x - 3)(x - 4)(x - 5).$$

Each of these factors is irreducible because it has degree 1.