§1	§2	§3	style	total

Math 415 Examination 3 Fall 2006

Modern Algebra I

Please print your **name**: Answer Key

1 True/false

Circle the correct answer; no explanation is required. Each problem in this section counts 5 points.

1. The rings $\mathbb{Z}_{15}$ and $\mathbb{Z}_3 \times \mathbb{Z}_5$ are isomorphic. `True` `False`

   Solution. True. This is a particular case of Example 18.15 on page 172 of the textbook.

2. The ring $\mathbb{Z} \times \mathbb{Z}$ is an integral domain. `True` `False`

   Solution. False. Since $(1,0)(0,1) = (0,0)$, the ring has zero divisors.

3. When 6^{14} is divided by 15, the remainder equals 1. `True` `False`

   Solution. False. Notice that 15 is not prime, and moreover 15 and 6 have a common factor, so the theorems of Fermat and Euler do not apply. Notice, however, that $6^2 = 36 \equiv 6 \mod 15$, so $6^{14} \equiv 6 \mod 15$, so the remainder when 6^{14} is divided by 15 equals 6.

4. $\mathbb{Q}[x]$ is a field of quotients of $\mathbb{Z}[x]$. `True` `False`

   Solution. False. The ring $\mathbb{Q}[x]$ is not even a field.

5. The polynomial $x^3 + x^2 + x + 1$ is reducible over $\mathbb{Q}$. `True` `False`

   Solution. True. By inspection, -1 is a zero of the polynomial, so $x+1$ is a factor. In fact, $x^3 + x^2 + x + 1 = (x+1)(x^2+1)$.

Modern Algebra I

2 Short answer

Fill in the blanks; no explanation is required. Each problem in this section counts 5 points.

6. In the direct product ring $\mathbb{Z}_5 \times \mathbb{Z}_9$, the product of the elements $(2, 3)$ and $(3, 4)$ equals _____ .

   Solution. Since $(2)(3) \equiv 1 \mod 5$ and $(3)(4) \equiv 3 \mod 9$, we have $(2, 3)(3, 4) = (1, 3)$ in $\mathbb{Z}_5 \times \mathbb{Z}_9$.

7. Solve the equation $5x = 2$ in the field $\mathbb{Z}_{31}$. $x =$ _____

   Solution. Working in the integers modulo 31, multiply by -6 to get $-30x \equiv -12 \mod 31$ or $x \equiv 19 \mod 31$. Thus $x = 19$ in $\mathbb{Z}_{31}$.

8. How many solutions does the equation $39x = 52$ have in the ring $\mathbb{Z}_{130}$?

   _____

   Solution. A corresponding problem in the integers is $39x = 52 + 130k$ for some integer k, or equivalently $3x = 4 + 10k$. Multiplying by 7 and reducing $\mod 10$ shows that the solutions in $\mathbb{Z}$ are the elements of the congruence class $8 + 10\mathbb{Z}$. Exactly 13 of these elements correspond to elements of $\mathbb{Z}_{130}$: namely, 8, 18, 28, ..., 128. Thus there are 13 solutions in $\mathbb{Z}_{130}$.

   One can also observe that $\gcd(39, 130) = 13$, and 13 divides 52, so Theorem 20.12 on page 187 applies.

9. How many zeroes does the quadratic polynomial $2x^2 + 4$ have in $\mathbb{Z}_6$?

   _____

   Solution. One can simply test all six elements of $\mathbb{Z}_6$ to see that 1, 2, 4, and 5 are zeroes, while 0 and 3 are not. Thus there are four zeroes.

   Notice that the number of zeroes exceeds the degree of the polynomial. This does not contradict Corollary 23.5 on page 212 because $\mathbb{Z}_6$ is not a field (indeed, $\mathbb{Z}_6$ is not even an integral domain). Unique factorization fails in the polynomial ring $\mathbb{Z}_6[x]$.

Modern Algebra I

10. The two tables show the binary operations of addition and multiplication for an integral domain of order 4. Fill in the four blanks.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b		1
b	b	a		0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		1
b	0	b		a

Solution. The addition table is a group table, so each row must contain each group element exactly once. Hence the missing entry in the bottom row must be 1, and the other missing entry must be 0.

By hypothesis, the multiplication operation is commutative, so the multiplication table must be symmetric. Therefore the missing entry in the bottom row of the multiplication table is 1. A finite integral domain is always a field (Theorem 19.11), so the part of the multiplication table obtained by deleting all the 0 entries is a group table; hence the remaining missing entry must be b. Another way to get that entry is to use the associative law: $bb = a$, so $aa = a(bb) = (ab)b = 1b = b$.

3 Essay questions

In the following problems, you must give an explanation. (Continue on the back if you need more space.) Each problem counts 15 points. In addition, this section as a whole carries 5 style points based on how well your solutions are written.

11. Suppose that R is a ring, and S is a non-empty subset of R that is closed under both multiplication and subtraction. In other words, whenever $a \in S$ and $b \in S$, it follows that both $ab \in S$ and $a - b \in S$. Show that S is a subring of R.

Modern Algebra I

Solution. This is essentially exercise 48 on page 176 of the textbook. Since S is closed under multiplication, all that needs to be checked is that S is a group under addition, because the commutative law for addition, the associative law for multiplication, and the distributive law all follow from the corresponding laws in R.

We know that a subset of a group is a subgroup if it contains the additive identity element, contains the additive inverse of each of its elements, and is closed under addition (Theorem 5.14). Let's check each of those properties for S.

Since S is non-empty, there exists some element a in S. Then by hypothesis, $a - a \in S$, that is, $0 \in S$. Now if b is any element in S, then by hypothesis $0 - b \in S$, that is, the additive inverse of b belongs to S. Finally, if a and b are any two elements of S, then $a - (-b) \in S$, that is, $a + b \in S$. This verifies the three necessary properties, so S is a subgroup of the additive group of R.

12. Suppose that R is a commutative ring, and S is a non-empty subset of R that is closed under multiplication (that is, whenever a and b are elements of S, then so is ab). Define a relation $\sim$ on the set $R \times S$ via

$$(r_1, s_1) \sim (r_2, s_2) \text{ if } s(r_1 s_2 - r_2 s_1) = 0 \text{ for some } s \text{ in } S.$$

Show that $\sim$ is an equivalence relation on $R \times S$.

Solution. This problem is closely related to the construction of the field of quotients in section 21 of the textbook. We need to check that the relation $\sim$ is reflexive, symmetric, and transitive.

For reflexivity, observe that if $r_1 = r_2$ and $s_1 = s_2$, then $s(r_1 s_2 - r_2 s_1) = s(r_1 s_1 - r_1 s_1) = 0$ for *every* element s in S (not just for some s). Hence $(r_1, s_1) \sim (r_1, s_1)$ when $r_1 \in R$ and $s_1 \in S$.

For symmetry, observe that if $s(r_1 s_2 - r_2 s_1) = 0$, then the additive inverse $s(r_2 s_1 - r_1 s_2)$ also equals 0. Hence if $(r_1, s_1) \sim (r_2, s_2)$, then also $(r_2, s_2) \sim (r_1, s_1)$.

For transitivity, suppose that $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$; we need to deduce that $(r_1, s_1) \sim (r_3, s_3)$. The two given relations imply the existence of elements s and s' in S such that $s(r_1 s_2 - r_2 s_1) = 0$ and $s'(r_2 s_3 - r_3 s_2) = 0$. Multiply the first equation by $s_3 s'$ and the second

equation by $s_1 s$ and add to get $s_2 s s'(r_1 s_3 - r_3 s_1) = 0$. Since the elements s_2, s, and s' all belong to S, and S is closed under multiplication, the element $s_2 s s'$ belongs to S. Therefore the preceding equation implies that indeed $(r_1, s_1) \sim (r_3, s_3)$.

13. If S is a subring of a ring R, then S is called an *ideal* if both $rs \in S$ and $sr \in S$ whenever $r \in R$ and $s \in S$. [Example: $R = \mathbb{Z}$ and $S = 2\mathbb{Z}$.] Show that the kernel of a ring homomorphism is always an ideal.

Solution. Let ϕ be a ring homomorphism from R to some ring. If $s \in \text{Ker}(\phi)$ (meaning that $\phi(s) = 0$) and $r \in R$, then the homomorphism property implies that $\phi(rs) = \phi(r)\phi(s) = \phi(r)0 = 0$ and $\phi(sr) = \phi(s)\phi(r) = 0\phi(r) = 0$. Hence $rs \in \text{Ker}(\phi)$ and $sr \in \text{Ker}(\phi)$.

It remains to check that $\text{Ker}(\phi)$ is a subring of R. Since in the preceding discussion the element r could, in particular, represent an arbitrary element of S, it follows from what has already been proved that $\text{Ker}(\phi)$ is closed under multiplication. Therefore we need only check that $\text{Ker}(\phi)$ is an additive subgroup of the additive group of R. But if we simply ignore the multiplicative structure, then ϕ is a group homomorphism of the underlying additive groups, and we know from group theory that the kernel of a group homomorphism is a subgroup (section 13).