Mathematics 351 – Abstract Algebra I
Solutions for Midterm Exam 2 – November 14, 2007

I. *Terminology.*

A) Let G be a group and n be an integer. What does it mean to say that $|g| = n$ for $g \in G$?

Solution: $|g|$ is the *order* of the element g. This is, by definition, the smallest positive integer such that $g^n = e$ (the identity element in G).

B) Let I be an ideal in a ring R. What does it mean to say that $a \equiv b \bmod I$?

Solution: This equivalent to saying $a - b \in I$.

C) Give an example of an ideal in a ring R that is prime but not maximal.

Solution: One such example is the ideal $P = \{(a, 0) : a \in \mathbb{Z}\}$ in $R = \mathbb{Z} \times \mathbb{Z}$. The quotient ring R/P is isomorphic to $\mathbb{Z}$, which is an integral domain but not a field. Hence P is a prime ideal, but not a maximal ideal.

II. Let R be the ring of functions $f : \mathbb{R} \to \mathbb{R}$ that have derivatives of all orders. Show that $I = \{f \in R : f(0) = f'(0) = 0\}$ is an ideal in R.

Solution: I is clearly nonempty since it contains the zero function, $f(x) = x^2$, etc. Let $f, g \in I$ so $f(0) = f'(0) = 0$ and $g(0) = g'(0) = 0$. Then $(f - g)(0) = f(0) - g(0) = 0$ and $(f - g)'(0) = f'(0) - g'(0) = 0 - 0 = 0$ (by the sum rule for derivatives). Hence $f - g \in I$. Next, let $f \in I$, and let g be any function in R. Since R is a commutative ring, we only need to check that $fg \in I$. But $(fg)(0) = f(0)g(0) = 0 \cdot g(0) = 0$. Moreover, by the product rule for derivatives,

$$(fg)'(0) = f'(0)g(0) + f(0)g'(0) = 0 \cdot g(0) + 0 \cdot g'(0) = 0.$$

Hence $fg \in I$.

III. All parts of this problem refer to $p(x) = x^2 + x$ in $\mathbb{Z}_2[x]$.

A) How many distinct cosets of the ideal $(p(x))$ are there in $\mathbb{Z}_2[x]$?

Solution: Since $\mathbb{Z}_2$ is a field, we have a division algorithm in the polynomial ring $\mathbb{Z}_2[x]$, and by our general results in this situation, the distinct cosets of $(p(x))$ are in one-to-one correspondence with the possible remainders on division by $p(x)$. Since $p(x)$ has degree 2, these remainders are all the polynomials of degree 1 or less in $\mathbb{Z}_2[x]$ (and the zero polynomial): $0, 1, x, x+1$. There are 4 distinct cosets:

$$0 + (p(x)), 1 + (p(x)), x + (p(x)), x + 1 + (p(x)).$$

B) Construct the coset addition and multiplication tables for the quotient ring $\mathbb{Z}_2[x]/(p(x))$.

Solution: The addition table (omitting the $+(p(x))$ in the description of the cosets for simplicity):

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

The multiplication table is:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	x	0
$x+1$	0	$x+1$	0	$x+1$

C) State and prove the First Isomorphism Theorem for rings.

Solution: The First Isomorphism states that if $f : R \to S$ is a ring homomorphism, then $\mathrm{im}(f) \simeq R/\ker(f)$. To prove this, we write $K = \ker(f)$ and consider the mapping $\phi : R/K \to \mathrm{im}(f)$ defined by $\phi(a + K) = f(a)$. This is well-defined since if $a + K = b + K$, then $a - b \in K$, so $f(a - b) = 0$, which shows $f(a) = f(b)$. Hence $\phi(a + K) = \phi(b + K)$. Next, we show that ϕ is a ring homomorphism. Let $a + K$ and $b + K$ be elements of R/K. Then $\phi((a + K) + (b + K)) = \phi((a + b) + K) = f(a + b) = f(a) + f(b) = \phi(a + K) + \phi(b + K)$. Similarly, $\phi((a + K) \cdot (b + K)) = \phi((a \cdot b) + K) = f(a \cdot b) = f(a) \cdot f(b) = \phi(a + K) \cdot \phi(b + K)$. (We are using the definition of the coset sum and product operations and the fact that f is a ring homomorphism here. Now, ϕ is onto $\mathrm{im}(f)$ by definition. Every element of $\mathrm{im}(f)$ is of the form $f(a)$ for some $a \in R$. Hence $f(a) = \phi(a + K)$. Finally, ϕ is one-to-one since if $\phi(a + K) = \phi(b + K)$, then $f(a) = f(b)$ which implies $f(a - b) = 0$ so $a - b \in K$, and hence $a + K = b + K$.

D) Let $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(a,b) : a,b \in \mathbb{Z}_2\}$, a ring under the component-wise sum and product operations. Show that $f : \mathbb{Z}_2[x] \to \mathbb{Z}_2 \times \mathbb{Z}_2$ defined by $f(g(x)) = (g(0), g(1))$ is a ring homomorphism and determine $\ker(f)$.

Solution: f is a ring homomorphism because

$$f(g(x)+h(x)) = (g(0)+h(0), g(1)+h(1)) = (g(0),g(1))+(h(0),h(1)) = f(g(x))+f(h(x))$$

and

$$f(g(x)\cdot h(x)) = (g(0)\cdot h(0), g(1)\cdot h(1)) = (g(0),g(1))\cdot(h(0),h(1)) = f(g(x))\cdot f(h(x)).$$

The kernel of f consists of all polynomials $g(x) \in \mathbb{Z}_2[x]$ such that $g(0) = 0$ and $g(1) = 0$. This means that x and $(x+1)$ must divide g, so $g(x) \in (p(x)) = (x(x+1))$. On the other hand every polynomial in $(p(x))$ is clearly in $\ker(f)$ since such polynomials are zero at $x = 0$ and $x = 1$. Hence $\ker(f) = (p(x))$.

E) Deduce that $\mathbb{Z}_2[x]/(p(x))$ is isomorphic as a ring to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution: This follows from part D by the First Isomorphism Theorem. Let f be as in part D. The image of f is all of $\mathbb{Z}_2 \times \mathbb{Z}_2$, so that is isomorphic to $\mathbb{Z}_2[x]/\ker(f)$ and $\ker(f) = (p(x))$. *Comment*: It is also possible to see this by comparing the addition and multiplication tables for the two rings. But it is necessary then to be somewhat careful in defining the correspondence between the elements. For example, the "obvious" mapping

$$\begin{aligned} 0+(p(x)) &\mapsto (0,0) \\ 1+(p(x)) &\mapsto (1,0) \\ x+(p(x)) &\mapsto (0,1) \\ x+1+(p(x)) &\mapsto (1,1) \end{aligned}$$

is an isomorphism of the additive groups of the two rings, but *not an isomorphism of rings* – note that the multiplicative identity in $\mathbb{Z}_2[x]/(p(x))$ is $1+(p(x))$, but the multiplicative identity in $\mathbb{Z}_2 \times \mathbb{Z}_2$ is $(1,1)$. A ring isomorphism would have to map the multiplicative identity to the multiplicative identity, so a correct mapping to get a ring isomorphism here is:

$$\begin{aligned} 0+(p(x)) &\mapsto (0,0) \\ 1+(p(x)) &\mapsto (1,1) \\ x+(p(x)) &\mapsto (0,1) \\ x+1+(p(x)) &\mapsto (1,0). \end{aligned}$$

This is the mapping obtained from f from part D by the proof of the First Isomorphism Theorem(!) There is also *another* correct way to do this by mapping

$$\begin{aligned} 0+(p(x)) &\mapsto (0,0) \\ 1+(p(x)) &\mapsto (1,1) \\ x+(p(x)) &\mapsto (1,0) \\ x+1+(p(x)) &\mapsto (0,1). \end{aligned}$$

IV. Let $G = \{4, 8, 12, 16\} \subset \mathbb{Z}_{20}$. Is G a group under *multiplication* mod 20? If so, say why and determine if G is cyclic. If not, identify which of the group axioms fail.

Solution: G is a group under multiplication mod 20, as can be seen from the operation table

$\cdot$	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

We see 16 is an identity for multiplication, every element has an inverse (that is, for each u, there is some v such that $uv = 16$), and associativity follows from associativity of multiplication in $\mathbb{Z}_{20}$. The group G *is cyclic*, since the powers of 8 generate all the elements: $8^1 = 8$, $8^2 = 4$, $8^3 = 12$, $8^4 = 16$.

V.

A) State Lagrange's Theorem for groups.

Solution: Lagrange's Theorem says that if G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. In particular, $|G| = [G : H]|H|$.

B) Let G be a group of order 60. Is it possible for G to contain elements a, b with $|a| = 3$ and $aba^{-1} = b^4$? Why or why not?

Solution: There certainly can be such elements. Note for instance that a cyclic group of order 60 generated by c will contain elements $a = c^{20}$ and $b = c^{40}$, both of order 3. Then $aba^{-1} = baa^{-1} = b = b^4$ since a and b commute and b also has order 3.