PRACTICE MIDTERM II

MATH 3140

Friday April 1, 2011.

Name | ______________________________

Please answer the all of the questions, and show your work.

1	2	3	4	5	
10	10	10	10	10	total

Date: March 29, 2011.

1
10 points

1. Let $R = \{a + bx : a, b \in \mathbb{C}\} \subseteq \mathbb{C}[x]$ be the set of polynomials of degree at most 1. Define addition and multiplication on R by

$$(a + bx) + (a' + b'x) = (a + a') + (b + b')x$$

and

$$(a + bx)(a' + b'x) = aa' + (ab' + a'b)x$$

for all $a, a', b, b' \in \mathbb{C}$. Show that $(R, +, \cdot)$ is a ring.

Solution. Let us begin by showing that $(R, +)$ is an abelian group. We have already shown that $\mathbb{C}[x]$ is an abelian group; next observe that the addition rule for R is the addition rule induced by that of $\mathbb{C}[x]$. So it will be enough to show that R is a subgroup of $\mathbb{C}[x]$. We have seen that it suffices to show that for all $a + bx, a' + b'x \in R$, we have $(a + bx) - (a' + b'x) \in R$. But we have

$$(a + bx) - (a' + b'x) = (a - a') + (b - b')x \in R$$

so indeed $(R, +)$ is a subgroup of $\mathbb{C}[x]$, (and hence a group).

Let us now check that $\cdot$ is an associative binary operation on R. For all $a, a', a'', b, b', b'' \in \mathbb{C}$ we have

$$\begin{gathered} ((a + bx)(a' + b'x))(a'' + b''x) = (aa' + (ab' + a'b)x)(a'' + b''x) \\ = (aa')a'' + (aa'b'' + (ab' + a'b)a'')x = (a + bx)(a'a'' + (a'b'' + a''b')x) \\ = (a + bx)((a' + b'x)(a'' + b''x)). \end{gathered}$$

Thus $\cdot$ is associative.

Finally, let us check that the distributive law holds. Since $\cdot$ is commutative, it suffices to show that for all $a, a', a'', b, b', b'' \in \mathbb{C}$, we have

$$(a + bx)((a' + b'x) + (a'' + b''x)) = (a + bx)(a' + b'x) + (a + bx)(a'' + b''x).$$

But a quick computation shows that both sides of the equality above are equal to

$$(aa' + aa'') + ((ab' + a'b) + (ab'' + a''b))x.$$

Thus the distributive law holds, and we have completed the proof that $(R, +, \cdot)$ is a ring. $\square$

2
10 points

2. Recall that for a commutative ring R with unity $1 \neq 0$, we define $R[x]$ to be the ring of polynomials in x with coefficients in R. Consider the map

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}_4[x] \quad \text{given by the rule} \quad \sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=0}^{n} [a_k] x^k.$$

2(a) [6 points]. Show that ϕ is a homomorphism of rings.

Solution. We must show for all $p(x), q(x) \in \mathbb{Z}[x]$ that

$$\phi(p(x) + q(x)) = \phi(p(x)) + \phi(q(x)) \quad \text{and} \quad \phi(pq) = \phi(p)\phi(q).$$

To do this, let us suppose that $p(x) = \sum_{k=0}^{n} a_k x^k$ and $q(x) = \sum_{j=0}^{m} b_j x^j$; since addition and multiplication is commutative, we may assume that $n \leq m$, and in fact, taking $a_k = 0$ for $k > n$, we may assume $n = m$. Then

$$\phi(p+q) = \phi\left(\sum_{k=0}^{n} a_k x^k + \sum_{j=0}^{n} b_j x^j\right) = \phi\left(\sum_{k=0}^{n} (a_k + b_k) x^k\right) = \sum_{k=0}^{n} [a_k + b_k] x^k$$
$$= \sum_{k=0}^{n} [a_k] x^k + \sum_{j=0}^{n} [b_j] x^j = \phi(p) + \phi(q).$$

Similarly,

$$\phi(p \cdot q) = \phi\left(\sum_{k=0}^{n} a_k x^k \cdot \sum_{j=0}^{n} b_j x^j\right) = \phi\left(\sum_{i=0}^{2n}\left(\sum_{k=0}^{i} (a_k b_{i-k})\right) x^i\right) = \sum_{i=0}^{2n}\left(\sum_{k=0}^{i} [a_k][b_{i-k}]\right) x^i$$
$$= \sum_{k=0}^{n} [a_k] x^k \cdot \sum_{j=0}^{n} [b_j] x^j = \phi(p) \cdot \phi(q).$$

Thus ϕ is a homomorphism of rings. □

2(b) [2 points]. Describe the kernel of ϕ (in terms of the coefficients of the polynomials).

Solution. We can describe the kernel as

$$\boxed{\ker \phi = 4\mathbb{Z}[x].}$$

Indeed, $p(x) = \sum_{k=0}^{n} a_k x^k \in \ker \phi \iff [a_k] = 0$ for all $k = 0, \ldots, n \iff a_k \in 4\mathbb{Z}$ for all $k = 0, \ldots, n$. □

2(c) [2 points]. Is ϕ surjective?

Solution. Yes, ϕ is surjective. If $g(x) = \sum_{k=0}^{n} [a_k] x^k \in \mathbb{Z}_4[x]$, then setting $p(x) = \sum_{k=0}^{n} a_k x^k$, we have $\phi(p) = g$. □

3
10 points

3. Let G be a group with center $Z(G)$. Assume that $G/Z(G)$ is cyclic.

3(a) [6 points]. Show that $Z(G) = G$. [Hint: Show there exists $g \in G$ such that for any $g_1 \in G$, there is a $z_1 \in Z(G)$ and $n_1 \in \mathbb{Z}$ such that $g_1 = g^{n_1} z_1$.]

Solution. It suffices to show that G is abelian (from the definition of the center, it follows immediately that G is abelian if and only if $G = Z(G)$). To show G is abelian, we must show that given $g_1, g_2 \in G$, then

$$g_1 g_2 = g_2 g_1.$$

To begin, since the group $G/Z(G)$ is cyclic, it has a generator $[g] \in G/Z(G)$ for some $g \in G$ (here I am using the notation $[g] = gZ(G)$). It follows that there are integers n_1, n_2 such that

$$[g_1] = [g]^{n_1} \text{ and } [g_2] = [g]^{n_2}.$$

We can rewrite this by saying that there exists $z_1, z_2 \in Z(G)$ such that $g_1 = g^{n_1} z_1$ and $g_2 = g^{n_2} z_2$. Then

$$g_1 g_2 = g^{n_1} z_1 g^{n_2} z_2 = g^{n_2} z_2 g^{n_1} z_1 = g_2 g_1$$

since by definition z_1, z_2 commute with all elements of G, and g commutes with itself. $\square$

3(b) [4 points]. Show that the commutator subgroup of G is trivial; i.e. $C(G) = \{e_G\}$.

Solution. This follows from the previous part of the problem. Indeed, it follows immediately from the definition of the commutator subgroup that $C(G) = e_G$ if and only if G is abelian. $\square$

4
10 points

4. Consider the dihedral group D_n, with $n \geq 3$. Recall the notation we have been using: D_n has identity element Id, and is generated by elements R and D, satisfying the relations $R^n = D^2 = Id$ and $RD = DR^{-1}$. Consider the cyclic subgroup $\langle R^2 \rangle$.

4(a) [6 points]. Show that $\langle R^2 \rangle$ is a normal subgroup of D_n.

Solution. To show that $\langle R^2 \rangle$ is normal in D_4, it suffices to check for all $g \in D_4$ that $g\langle R^2 \rangle g^{-1} \subseteq \langle R^2 \rangle$. (For a subgroup H of a group G, we have seen that H is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$). So let $R^{a_1}D^{b_1} \in D_4$ and let $R^{2k} \in \langle R^2 \rangle$ (here $k \in \mathbb{Z}$). Then

$$R^{a_1}D^{b_1}R^{2k}(R^{a_1}D^{b_1})^{-1} = R^{a_1}D^{b_1}R^{2k}D^{b_1}R^{-a_1} = R^{a_1}D^{b_1}D^{b_1}R^{(-1)^{b_1}2k}R^{-a_1} = R^{(-1)^{b_1}2k} \in \langle R^2 \rangle.$$

Thus $\langle R^2 \rangle$ is normal in D_n. $\square$

4(b) [4 points]. Find the order of the group $D_n/\langle R^2 \rangle$ [Hint: this may depend on the parity of n.]

Solution.

$$\boxed{|D_4/\langle R^2 \rangle| = 2 \text{ if } n \text{ is odd, and } 4 \text{ if } n \text{ is even.}}$$

To see this, we note that the order of R in D_n is n. Consequently, if n is odd, then $\langle R^2 \rangle = \langle R \rangle$, which has order n. If n is even, then $\langle R^2 \rangle \neq \langle R \rangle$ and the order of $\langle R^2 \rangle$ is $n/2$. By Lagrange's Theorem, the order of $D_4/\langle R^2 \rangle$ is then $2n/n = 2$ if n is odd, or $2n/(n/2) = 4$ if n is even. $\square$

5
10 points

5. True or false. (Please provide a sentence or two of explanation.)

5(a). If G is a group of order n and k divides n, then G has a subgroup of order k.

Solution. FALSE: we have seen that A_4 has order 12, but does not have a subgroup of order 6. □

5(b). The alternating group A_5 is simple.

Solution. TRUE: this was a homework exercise. □

5(c). The kernel of a homomorphism is a normal subgroup.

Solution. TRUE: this is a theorem we proved. □

5(d). Every element in a ring has an additive inverse.

Solution. TRUE: if $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group. □

5(e). Let R be a ring, and let $a \in R$. If $a^2 = a$, then $a = 0_R$ or $a = 1_R$.

Solution. FALSE: See for instance Exercise 18.56 (and 18.55); these give examples of rings R (called Boolean rings) where every element $a \in R$ (including $a \neq 0_R$, $a \neq 1_R$) satisfies $a^2 = a$. □