PRACTICE FINAL

MATH 3140

1:00 PM Wednesday April 27, 2011 to 1:00 PM Friday April 29, 2011

Name

Please answer the all of the questions, and show your work. You must **hand your exam to me in person**, in class on Friday (do not leave your exam in a mailbox or under my door). You may consult your textbook, your class notes, your homework, your exams, the three practice exams, and **nothing else**. Do not discuss the exam with anyone except for me.

1	2	3	4	5	6		
10	10	10	10	10	10	total	percent

Date: April 25, 2011.

1
10 points

1. Let $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$.

1(a) [3 points]. Show that $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$.

1(b) [3 points]. Show that $(x^2 + 1) := \{(x^2 + 1)g(x) : g(x) \in \mathbb{Q}[x]\}$ is an ideal in $\mathbb{Q}[x]$.

1(c) [4 points]. It is a fact that any ideal I in $\mathbb{Q}[x]$ such that $(x^2 + 1) \subseteq I \subseteq \mathbb{Q}[x]$ is either equal to $(x^2 + 1)$ or $\mathbb{Q}[x]$. Use this to show that $\mathbb{Q}[i]$ is isomorphic to the quotient ring $\mathbb{Q}[x]/(x^2 + 1)$. [Hint: consider an evaluation homomorphism.]

Solution. 1(a). Let us show that $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$. To begin, it is a subgroup. Indeed, if $(a_1 + b_1 i), (a_2 + b_2 i) \in \mathbb{Q}[i]$ then

$$(a_1 + b_1 i) - (a_2 + b_2 i) = (a_1 - a_2) + (b_1 - b_2)i \in \mathbb{Q}[i].$$

(We are using the fact that a subset H of a group G is a subgroup if and only if for all $h_1, h_2 \in H$, we have $h_1 h_2^{-1} \in H$.) Now let us check that $\mathbb{Q}[i]$ is closed under multiplication. We have

$$(a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i \in \mathbb{Q}[i].$$

Thus $\mathbb{Q}[i]$ is closed under multiplication. The remaining conditions in the definition of a ring (associativity of multiplication, and the distribution laws) hold, since they hold on $\mathbb{C}$. Thus $\mathbb{Q}[i]$ is a subring of $\mathbb{C}$.

Let us now check that $\mathbb{Q}[i]$ is a field. First, $\mathbb{Q}[i]$ contains $1 = 1 + 0i$. Moreover, for any non-zero element $a + ib \in \mathbb{Q}[i]$ we have

$$(a + ib)^{-1} = (a^2 + b^2)^{-1}(a - ib) \in \mathbb{Q}[i].$$

Thus we have shown that $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$.

1(b). We intend to show that $(x^2 + 1)$ is an ideal in $\mathbb{Q}[x]$. First let us check it is a subgroup. Let $(x^2 + 1)g_1(x), (x^2 + 1)g_2(x) \in (x^2 + 1)$. Then

$$(x^2 + 1)g_1(x) - (x^2 + 1)g_2(x) = (x^2 + 1)(g_1(x) - g_2(x)) \in (x^2 + 1).$$

Thus $(x^2 + 1)$ is a subgroup of $\mathbb{Q}[x]$. Let us now check that it is an ideal. Let $f(x) \in \mathbb{Q}[x]$ and let $(x^2 + 1)g(x) \in (x^2 + 1)$. Then

$$((x^2 + 1)g(x))f(x) = f(x)((x^2 + 1)g(x)) = (x^2 + 1)(f(x)g(x)) \in (x^2 + 1).$$

Thus $(x^2 + 1)$ is an ideal in $\mathbb{Q}[x]$.

1(c). We will show that $\mathbb{Q}[i]$ is isomorphic to $\mathbb{Q}[x]/(x^2 + 1)$. To do this, consider the evaluation homomorphism at $i \in \mathbb{Q}[i]$:

$$\phi : \mathbb{Q}[x] \to \mathbb{Q}[i]$$

given by $\phi(f(x)) = f(i)$ (We have proven in class that evaluation maps give homomorphisms). It is obvious that $(x^2 + 1) \subseteq \ker \phi$. Now let us show the other inclusion.

We do this using the fact mentioned in the statement of the problem. Indeed, from this fact, we can conclude that $\ker\phi$ is either equal to (x^2+1) or to all of $\mathbb{Q}[x]$. In the latter case, the evaluation homomorphism would be the zero homomorphism, which is a contradiction. Thus we conclude that $\ker\phi = (x^2+1)$.

Finally, note also that ϕ is surjective. Indeed for any $a+ib \in \mathbb{Q}[i]$ we have $\phi(a+ix) = a+ib$. Now since ϕ is surjective, with kernel equal to (x^2+1), it follows from the fundamental homomorphism theorem for rings that $\mathbb{Q}[i] \cong \mathbb{Q}[x]/(x^2+1)$. $\square$

2
10 points

2(a) [2 points]. Let R be a ring with unity 1_R, let R' be a ring with no zero divisors, and let $\phi : R \to R'$ be a non-zero homomorphism. Show that R' has a multiplicative identity element equal to $\phi(1_R)$.

2(b) [4 points]. Find all ring homomorphisms from $\mathbb{Z}_p$ to $\mathbb{Z}_p$.

2(c) [4 points]. Find all ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Q}$.

Solution. 2(a). Let R be a ring with unity 1_R, let R' be a ring with no zero divisors, and let $\phi : R \to R'$ be a non-zero homomorphism. We must show that R' has multiplicative identity equal to $\phi(1_R)$. That is to say, we must show that for all $r' \in R'$, we have $\phi(1_R)r' = r'\phi(1_R) = r'$. To do this, first observe that $\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R)$. Then starting with $r' - r' = 0_{R'}$, we have

$$\phi(1_R)r' - \phi(1_R)r' = 0_{R'} = r'\phi(1_R) - r'\phi(1_R).$$

Using the observation, we get

$$\phi(1_R)\phi(1_R)r' - \phi(1_R)r' = 0_{R'} = r'\phi(1_R)\phi(1_R) - r'\phi(1_R).$$

Consequently, we see

$$\phi(1_R)\left[\phi(1_R)r' - r'\right] = 0_{R'} = \left[r'\phi(1_R) - r'\right]\phi(1_R).$$

Since R' has no zero divisors, this implies that either $\phi(1_R) = 0_{R'}$, or $\phi(1_R)r' = r'\phi(1_R) = r'$. But in the former case, we would have ϕ being the zero homomorphism, since $\phi(r) = \phi(1_R \cdot r) = 0_{R'} \cdot \phi(r) = 0_{R'}$ for all $r \in R$. Thus it must be the case that $\phi(1_R)r' = r'\phi(1_R) = r'$ for all $r' \in R'$. In other words, $\phi(1_R)$ is the multiplicative identity for R'.

2(b). **A homomorphism of rings $\phi : \mathbb{Z}_p \to \mathbb{Z}_p$ is either the zero homomorphism, or the identity**. To see this, let $\phi : \mathbb{Z}_p \to \mathbb{Z}_p$ be a non-zero ring homomorphism. From part (a) we may conclud that $\phi(1) = 1$. This in fact determines $\phi(n)$ for all $n \in \mathbb{Z}_p$. Indeed, we have

$$\phi(n) = \phi(\underbrace{1 + \cdots + 1}_{n}) = n \cdot \phi(1) = n \cdot 1 = n.$$

In other words, if ϕ is not the zero homomorphism, then it is the identity.

2(c). **Any homomorphism of rings $\phi : \mathbb{Q} \to \mathbb{Q}$ is either the zero homomorphism, or the identity**. The proof is similar to the proof of part (b). Again from part (a) we may conclude that $\phi(1) = 1$. The same argument as in part (b) then shows that for all $n \in \mathbb{Z}$, $\phi(n) = n$. Now any rational number $q \in \mathbb{Q}$ can be written as $q = nd^{-1}$ for some $n, d \in \mathbb{Z}$. Thus

$$\phi(q) = \phi(nd^{-1}) = \phi(n)\phi(d^{-1}) = \phi(n)\phi(d)^{-1} = nd^{-1} = q.$$

In other words, if ϕ is not the zero homomorphism, then it is the identity. $\square$

3
10 points

3(a) [2 points]. In a commutative ring with unity, show that $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ for all a, b in the ring. [Hint: First show that $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$, then use induction.]

3(b) [8 points]. An element r of a ring R is said to be nilpotent if there exists some $n \in \mathbb{N}$ such that $r^n = 0$. Let N be the set of nilpotent elements of a commutative ring R with unity. Show that N is an ideal in R.

Solution. 3(a). Following the hint, let us first check that indeed $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. The computation is

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(n-k+1)!(k-1)!} + \frac{n!}{(n-k)!k!} = \frac{n!k}{(n-k+1)!k!} + \frac{n!(n-k+1)}{(n-k+1)!k!}$$
$$= \frac{(n+1)!}{(n+1-k)!k!} = \binom{n+1}{k}.$$

Now we will use this observation to prove the problem using induction. We start with the case $n = 1$, and we check that

$$\sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k} = b + a = (a+b)^1.$$

We now perform the inductive step. We assume that $(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k}$ for all $m \leq n$ for some $n \geq 1$. We then must show that

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

Here is the computation:

$$(a+b)^{n+1} = (a+b)^n(a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) (a+b),$$

where the second equality follows from the inductive hypothesis. Now, using the distributive law, we have that this is equal to

$$= \left(\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} \right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \right).$$

Pulling out the first term on the left, the last term on the right, and combining the rest, we see that this is equal to

$$= \binom{n}{0} b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} + \binom{n}{n} a^{n+1}.$$

We now use the fact that $\binom{m}{0} = \binom{m}{m} = 1$ for any $m \in \mathbb{N}$, as well as the observation in the hint to rewrite this as

$$= \binom{n+1}{0} b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + \binom{n+1}{n+1} a^{n+1}.$$

Recombining all of the terms into one sum, we finally have that this is equal to

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

This completes the final step of the inductive proof. Thus we may conclude that for all $n \in \mathbb{N}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

3(b). We must show the set N of nilpotents of the commutative ring with unity R form an ideal. First we will show that the set of nilpotents is a subgroup. Let $a, b \in N$; we will show that $(a - b) \in N$. To do this, suppose that $\alpha, \beta \in \mathbb{N}$ are such that $a^\alpha = b^\beta = 0_R$; note that $(-b)^\beta = (-1)^\beta b^\beta = 0$ as well. Let n be an integer such that $n > \alpha + \beta$. Then using part (a), we have

$$(a + (-b))^n = \sum_{k=0}^{n} \binom{n}{k} a^k (-b)^{n-k} = 0$$

since either $k > \alpha$ or $n - k > \beta$ (otherwise $n = k + (n - k) < \alpha + \beta$). Thus $a - b \in N$, and N is a subgroup.

To show that it is an ideal, let $r \in R$ and $a \in N$. Let $n \in \mathbb{N}$ be such that $a^n = 0$. Then $(ar)^n = (ra)^n = r^n a^n = 0$, so that $ra \in N$. Thus N is an ideal. $\square$

4
10 points

4. Show that for a prime p, $x^p + a \in \mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$.

Solution. By Fermat's Little Theorem, we know that $b^p = b$ for all $b \in \mathbb{Z}_p$. Thus $-a$ is a root of $x^p + a$ in $\mathbb{Z}_p$. It follows (from a theorem we proved in class) that $(x + a)$ is an irreducible factor of $x^p + a$ in $\mathbb{Z}_p[x]$. Thus $x^p + a$ is not irreducible for any $a \in \mathbb{Z}_p$. $\square$

5
10 points

5. Show that a finite, simple, abelian group has prime order. [Hint: use the Fundamental Theorem of Finitely Generated Abelian Groups.]

Solution. Let G be a finite, simple, abelian group. We must show that G has prime order. Since G is simple, and any subgroup of an abelian group is normal, we may assume that G has no non-trivial proper subgroups. Since G is abelian, by the Fundamental Theorem of Finitely Generated Abelian Groups, there is an isomorphism

$$G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_m}$$

for some $m, n_1, \ldots, n_m \in \mathbb{N}$. We may assume all the $n_i \geq 2$ since G is non-trivial (this is part of the definition of simple). If $m > 1$, then there is a proper, non-trivial subgroup $\mathbb{Z}_{n_1} \times \{0\} \times \ldots \times \{0\}$. Thus $m = 1$. In addition, any number $n \in \mathbb{N}$ dividing n_1, with $n \neq 1, n_1$ determines a proper, non-trivial subgroup of order n_1/n in $\mathbb{Z}_{n_1}$. Thus n_1 must be prime. The order of $\mathbb{Z}_{n_1}$ is n_1, and so $|G| = n_1$ is prime. $\square$

6
10 points

6. True or false.

6(a). A quotient ring of an integral domain is an integral domain.

.... F. For example $\mathbb{Z}/4\mathbb{Z}$.

6(b). Every quotient group of a cyclic group is cyclic.

.... T. We have seen that a group G is cyclic if and only if it admits a surjective homomorphism from $\mathbb{Z}$. A quotient group G/N admits a surjective homomorphism from G, and a composition of surjective homomorphisms is a surjective homomorphism. I.e. $\mathbb{Z} \to G \to G/N$ is surjective.

6(c). Let $n \in \mathbb{N}$. There is a single group G of order $n!$ such that any finite group of order n is isomorphic to a subgroup of G.

.... T. Every finite group of order n is isomorphic to a subgroup of S_n. This is Cayley's theorem.

6(d). Let p and q be primes. A proper subgroup of a group of order pq is cyclic.

.... T. By Lagrange's Theorem, such a proper subgroup will have order 1, p or q. Every group of prime order is cyclic; and the trivial group is cyclic.

6(e). The characteristic of a ring is a prime number.

.... F. For example $\mathbb{Z}/4\mathbb{Z}$.

6(f). The direct product of two fields is a field.

.... F. If F, F' are fields, then in $F \times F'$, we have $(1,0) \cdot (0,1) = (0,0)$. Thus the direct product of fields will not even be an integral domain, let alone a field.

6(g). For a prime p, and an integer z, we have $z^p \equiv z \pmod{p}$.

.... T. This is a consequence of Fermat's Little Theorem.

6(h). If R is a ring, then the zero divisors of $R[x]$ are precisely the zero divisors of R.

.... F. For example in $\mathbb{Z}_4[x]$ we have $(2+2x)(2+2x) = 4 + 8x + 4x^2 = 0$.

6(i). The polynomial $x^7 - 2$ is irreducible over $\mathbb{Q}$.

.... T. Use for instance Eisenstein's Criterion with $p = 2$.

6(j). If F is a field, then there exist irreducible polynomials in $F[x]$ of every positive degree.

.... F. $\mathbb{C}$; in $\mathbb{C}[x]$ there are no irreducible polynomials of degree greater than one.