HOMEWORK # 9
DUE WEDNESDAY MARCH 30TH

MATH 435 SPRING 2011

In this homework assignment, all rings with be commutative associative with unity (multiplicative identity). Ring homomorphisms will always be assumed to send 1 to 1. The terms that appear on this homework assignment *WILL* appear on the exam.

1. An ideal I is called *radical* if for every $x \in R$ such that $x^n \in I$ (for some n), then $x \in I$ also. Prove that I is radical if and only if R/I has no *nonzero* nilpotent elements.

Solution: First suppose that I is radical and that $x+I \in R/I$ is a nilpotent element. Then $x^n+I = (x+I)^n = 0_{R/I} = 0+I \in R/I$. Thus $x^n+I = 0+I$ and so $x^n \in I$. But then since I is radical, $x \in I$, so that $x+I = 0+I$. Therefore, the only nilpotent element of R/I is the zero element (of R/I).

Conversely, suppose that I is not radical. Thus there exists $x \in R$, such that $x \notin I$ but $x^n \in I$ for some positive integer n. Thus $x+I \neq 0+I$ but $x^n+I = 0+I$. However, $(x+I)^n = x^n+I = 0+I = 0_{R/I}$ proving that $x+I$ is a non-zero nilpotent element.

2. Suppose that $x \in R$ is a nilpotent element. Prove that $1+x$ is a unit.

Solution: Suppose $x^n = 0$ for some integer $n > 0$. Then

$$(1+x)(1-x+x^2-x^3+x^4-\cdots+(-1)^{n-1}x^{n-1}) = 1+(-1)^{n-1}x^n = 1.$$

This proves that $1+x$ is a unit.

3. Suppose that I and J are ideals of a ring. We define $IJ = \{x \in R | x \text{ is equal to a finite sum of } ij \text{ for some } i \in I, j \in J\}$. Show that both IJ and $I \cap J$ are ideals of R. Further show that $IJ \subseteq I \cap J$.

Solution: Suppose we have $x = i_1j_1+\cdots+i_nj_n \in IJ$ and $x' = i'_1j'_1+\cdots+i'_nj'_n$. Then $x+x' = i_1j_1+\cdots+i_nj_n+i'_1j'_1+\cdots+i'_nj'_n \in IJ$. Likewise if $r \in R$, then $rx = ri_1j_1+\cdots+ri_nj_n = (ri_1)j_1+\cdots+(ri_n)j_n \in IJ$ since I is an ideal (and so $rI \subseteq I$). These two properties prove that IJ is an ideal. Furthermore, each term of $x = i_1j_1+\cdots+i_nj_n$ is an element of I (they are all multiples of elements of i). Likewise each term is in J. Thus $x \in I$ and $x \in J$ (since ideals are closed under addition). In conclusion, $x \in I \cap J$, and so $IJ \subseteq I \cap J$ as desired.

4. A ring R is called a *principal ideal domain* if it is an integral domain and every ideal $I \subseteq R$ is principal, in other words $I = (r)$ for some R in R. Show that $\mathbb{Z}[i]$ is a principal ideal domain.

Solution: See Theorem 3.59 in Rotman.

5. Consider the ring R of continuous functions $\phi : \mathbb{R} \to \mathbb{R}$. Prove that the subset $I = \{f \in R | f(1) = 0\}$ is an ideal but that $A = \{f \in R | f(1) \in \mathbb{Z}\}$ is not an ideal.

Solution: Suppose $g \in R$ and $f \in I$. Then $(gf)(1) = g(1)f(1) = g(1)0 = 0$ so that $gf \in I$ as well. Suppose $f_1, f_2 \in I$, then $(f_1+f_2)(1) = f_1(1)+f_2(2) = 0+0 = 0$. Thus I is an ideal.

Now for the second part, consider the function $g \in R$ which is the constant function $g(x) = 1/2$. Consider the constant function $f \in A$ defined by $f(x) = 1$. Then $(gf)(1) = g(1)f(1) = (1/2)(1) = (1/2) \notin \mathbb{Z}$.

6. Suppose that A is an integral domain of positive characteristic. Suppose that $I \subsetneq A$ is an ideal. Prove that A/I has the same characteristic as A. However, give an example which demonstrates that A/I need not be an integral domain.

Solution: Since A is an integral domain, A has prime characteristic $p > 0$. Since I is not equal to A, $1+I \in A/I$ is not the zero element (in other words, $1+I \neq 0+I$). We know $p1 = 0 \in A$. Therefore also $p(1+I) = p1+I = 0+I$

in A/I. Thus the characteristic of A/I is less than or equal to the characteristic of A. Suppose it is strictly less than. We consider the cyclic group generated by $1+I$ as a subgroup (under addition) of A/I. We know that the order of $1+I$ divides p by Lagrange's theorem. The order of $1+I$, under addition, is also not equal to 1 since $1+I \neq 0+I$. Thus since p is prime, the order of $1+I$ is equal to p. But the order of $1+I$ is the same as the characteristic of A/I. This completes the proof.

7. Suppose that F is a field with finitely many elements but not with only 2 elements (ie, not isomorphic to $\mathbb{Z}_{\text{ mod } 2}$). Prove that the sum of all the elements in the field is equal to zero.

Solution: In an earlier version of the homework, I didn't rule out $\mathbb{Z}_{\text{ mod } 2}$. Obviously that won't work. Consider now $h = \sum_{x \in F} x = \sum_{0 \neq x \in F} x$. Choose an element $x \in F$ which is not zero and not equal to 1 (we are using the fact that $\mathbb{Z}_{\text{ mod } 2} \neq F$). Now, the elements $F \setminus \{0\}$ form a group under multiplication, so multiplication by x permutes the elements of $F \setminus \{0\}$. Therefore, $xh = h$. In particular, because h is a field and thus an integral domain, $h(x-1) = 0$. Since x is not 1, we must have that $h = 0$ as desired.

8. Find the characteristic of $\mathbb{Z}[i]/(2+i)$.

Solution: The characteristic to $\mathbb{Z}[i]/(2+i)$ is 5. To see this, we first have to prove that $1+(2+i)$ is not equal to zero. In other words, suppose that there exists $a+bi \in \mathbb{Z}[i]$ such that $1 = (a+bi)(2+i)$, in other words that $(a+bi) = 1/(2+i) \in \mathbb{Z}[i]$. However, $1/(2+i) = (2-i)/\left((2-i)(2+i)\right) = (2-i)/5 = 2/5 - i/5$. But this is clearly not in $\mathbb{Z}[i]$. Thus $1+(2+i) \neq 0+(2+i)$. On the other hand $5(1+(2+i)) = 5+(2+i) = (2+i)(2-i)+(2+i) = 0+(2+i)$. Therefore the characteristic of $\mathbb{Z}[i]/(2+i)$ is less than or equal to 5, and furthermore, by the argument of **6.**, we see that the characteristic divides 5. But since $1+(2+i) \neq 0+(2+i)$, the characteristic is > 1, and so the characteristic is indeed 5.

9. Give an example of a prime ideal which is not maximal. An ideal $I \subseteq R$ is called *maximal* if there are no proper ideals J such that $I \subsetneq J \subsetneq R$.

Solution: The ideal (0) in $\mathbb{Z}$ is not maximal (the ideal (2) contains it), but it is prime (note that a ring is an integral domain if and only if the zero ideal (0) is prime).

10. Show that the ideal $(2+\sqrt{2}) \subseteq \mathbb{Z}[\sqrt{2}]$ is not prime.

Solution: As stated, this problem is *false*. In fact $(2+\sqrt{(2)})$ is prime! I think I intended to ask that either $2+2\sqrt{2}$ is *not prime*, or that 2 is *not prime*.

In the former, we can factor $2+2\sqrt{2} = 2(1+\sqrt{2}) = (2+\sqrt{2})(2-\sqrt{2})(1+\sqrt{(2)})$. One would then have to show that two of those elements are not a unit (notice that $1/(1+\sqrt{2}) = (1-\sqrt{2})/(1^2-2) = -1+\sqrt{2}$ so $1+\sqrt{2}$ is a unit). On the other hand $2+\sqrt{2}$ is not a unit since $\frac{1}{2+\sqrt{2}} = \frac{2-\sqrt{2}}{2} = 1 - \frac{1}{2}\sqrt{2} \notin \mathbb{Z}[\sqrt{2}]$. Likewise $2-\sqrt{2}$ is not a unit since $\frac{1}{2-\sqrt{2}} = \frac{2+\sqrt{2}}{2} = 1+\frac{1}{2}\sqrt{2} \notin \mathbb{Z}[\sqrt{2}]$. Thus $(2+\sqrt{2})$ is not irreducible and thus also not prime.

In fact, the argument above also shows that 2 is not irreducible, and therefore also not prime, showing the latter condition.

11. Suppose that S is a ring. Show that there is a unique ring homomorphism $\phi : \mathbb{Z} \to S$ which sends 1 to 1. In particular, conclude that there is only one ring homomorphism $\mathbb{Q} \to \mathbb{Q}$ which sends 1 to 1.

Solution: Suppose $\phi(1) = 1$. Then $\phi(n) = \phi(\sum_{i=1}^n 1) = \sum_{i=1}^n \phi(1) = n\phi(1) = n$. In particular, ϕ is forced to be the identity homomorphism. Of course, the identity homomorphism exists, so we have shown that there exists a *unique* homomorphism with the desired property.

Conversely, now consider a ring homomorphism $\phi : \mathbb{Q} \to \mathbb{Q}$ which sends 1 to 1. By the above work, it must also send n to n. Now $n = \phi(n) = \phi(nm/m) = \phi(m)\phi(n/m) = m\phi(n/m)$. Thus solving for $\phi(n/m)$ yields $\phi(n/m) = n/m$. Thus the only such homomorphism is again the identity homomorphism.

12. Fix a field k and consider the subring $R = k[x^2, x^3] \subseteq k[x]$ (the former ring is all polynomials with zero coefficient in front of x). Prove that $k[x^2, x^3]$ is not a principal ideal domain.

Solution: We will show that the ideal (x^2, x^3) is not principal. Suppose it were principal, then $(x^2, x^3) = (f)$ for some $f \in k[x^2, x^3]$. Now, $x^2, x^3 \in (f)$ so $f|x^2$ and $f|x^3$. Of course, all the elements involved are in $k[x]$. Then since $f|x^2$ there are three possibilities, $f = \lambda$ for some non-zero $\lambda \in k$, or $f = \lambda x$, or $f = \lambda x^2$. The first case is impossible since then $(f) = R$, but $(x^2, x^3)_R \neq R$ since even $(x^2, x^3)_{k[x]} = (x^2)$ does not contain 1. The second case is impossible since then $f \not| R$. This leaves only the final case. Thus $f = \lambda x^2$. But $f | x^3$, so $\lambda x^2 | x^3$. In other words, there exists $r \in R$ such that $r\lambda x^2 = x^3$. Again, all these elements live in $k[x]$ which forces $r = \frac{1}{\lambda}x$. But again, this is impossible since $r = \frac{1}{\lambda}x \notin R$. Thus all possibilities lead to a contradiction and so our assumption that (x^2, x^3) is principal must be false.

13. Suppose that $\phi : R \to S$ is a surjective ring homomorphism. Prove that if R is a principal ideal domain the every ideal in S is also principal. However, give an example to show that S need not be an integral domain.

Solution: First we suggest that the reader search the text to find a proof of the fact that $f^{-1}(I)$ is an ideal of R for every ideal $I \subseteq S$.

Now we attack the proof. Suppose $I \subseteq S$ is indeed an ideal of S, we will show that I is principal. However, because R is a PID, $\phi^{-1}(I) = (g)_R$ for some $g \in R$. Because ϕ is surjective, $\phi(\phi^{-1}(I)) = I$ (I leave as an exercise to the reader, but it is merely a fact about functions between sets, and has nothing to do with rings). Thus every element of I is of the form $\phi(h)$ for some $h \in (g)$. But all such h are of the form $h = rg$. Thus every element of I has the form $\phi(rg) = \phi(r)\phi(g)$. In particular, they are all multiples of g. However, because r is allowed to be arbitrary and ϕ is surjective, all $s \in S$ appear as $s = \phi(r)$. Thus $\phi(\phi^{-1}(I)) = (\phi(g))_S$ and so it is principal as well.

For the example, consider $\phi : \mathbb{Z} \to \mathbb{Z}_{\text{ mod } 4}$ with the obvious surjective map $\phi(n) = n \mod 4$. This map is surjective, but $\mathbb{Z}_{\text{ mod } 4}$ is certainly not an integral domain.

14. Let $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} | a, b \in \mathbb{Q}\}$ Prove that both rings are fields but that they are not isomorphic.

Solution: First we show that $\mathbb{Q}[\sqrt{2}]$ is a field. All these rings are subrings of $\mathbb{R}$ so we do some of our computations there. First suppose that $a + b\sqrt{2}$ is non-zero (meaning either a or b is non-zero, possibly both being non-zero). Then

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a - b\sqrt{2}} \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{5} \in \mathbb{Q}[\sqrt{2}]$$

as desired. This work shows that non-zero element has an inverse as long as $a^2 - 2b^2 \neq 0$. To show this last step, suppose $a^2 - 2b^2 = 0$, then $a^2 = 2b^2$. If $b = 0$, then automatically $a = 0$ which is a contradiction to our assumptions. If $b \neq 0$, then $(a/b)^2 = 2$, proving that $\sqrt{2} = a/b \in \mathbb{Q}$. But $\sqrt{2}$ is irrational.

Likewise, we show that $\mathbb{Q}[\sqrt{5}]$ is a field. Again notice that

$$\frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{a - b\sqrt{5}} \frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{a^2 - 5b^2} = \frac{a}{a^2 - 5b^2} - \frac{b}{a^2 - 5b^2}\sqrt{5} \in \mathbb{Q}[\sqrt{5}].$$

Similar arguments as above prove that this element has non-zero denominators and so does really make sense. Thus both rings are fields.

Now we show that the two fields are not isomorphic. Suppose that $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$ was indeed a ring isomorphism. By the argument above in **11.**, $\phi(2) = 2$. Thus $\left(\phi(\sqrt{2})\right)^2 = \phi(\sqrt{2}\sqrt{2}) = \phi(2) = 2$. Therefore, 2 is a perfect square in $\mathbb{Q}[\sqrt{5}] = \{a+b\sqrt{5} | a, b \in \mathbb{Q}\}$. So suppose $\phi(\sqrt{2}) = a+b\sqrt{5}$. Then $2 = (a+b\sqrt{5})^2 = a^2+2ab\sqrt{5}+5b^2$. In particular, $2 - a^2 - 5b^2 = 2ab\sqrt{5}$. Obviously the left side is a rational number, and so the right side is a rational number as well. But that can only happen if a or b is zero. Thus we have two cases.

Case 1. $a = 0$, then $2 = 0^2 + 20b\sqrt{5} + 5b^2 = 5b^2$ which implies that $2/5$ is a perfect square which is ridiculous. Case 2. $b = 0$ which implies that $2 = a^2$ which again is ridiculous. Thus both cases lead to contradiction and so the two field cannot be isomorphic.