Modern Algebra II: Problem Set 4

Nilay Kumar

Last updated: February 17, 2013

Problem 1

Let R be a ring with $R \neq \{0\}$. We wish to show that R is a field if and only if every ideal of R is either $\{0\}$ or R. If R is a field, we know that every nonzero $r \in R$ has an inverse r^{-1}. Take any ideal $I \subset R$. If I is empty, we are done. Otherwise, I contains at least one element, call it r. By the ideal's absorbing property, $rr^{-1} = 1$ must also be in I. However, we know that if I contains 1, it must contain the whole ring R, and we are done.

Conversely, let R be a ring with ideals only $\{0\}$ and R. We wish to show that every non-zero element R has a multiplicative inverse, r^{-1}. Take the ideal generated by some $r \in R$: $(r) = \{rs | s \in R\}$. By hypothesis, $(r) = \{0\}$ or $(r) = R$. We are not interested in the former case, as it requires that $r = 0$. If $(r) = R$, on the other hand, (r) must contain unity, i.e. 1 can be written as a multiple of r. It follows, then, that $rs = 1$ for some $s \in R$, and thus we have found a multiplicative inverse for any non-zero element $r \in R$, and thus R must be a field.

Problem 2

Let F be a field and let $\rho : F \to R$ be a ring homomorphism. We wish to show that either ρ is injective or $R = \{0\}$ and hence $\rho(a) = 0$ for all $a \in F$.

Since $\ker \rho$ is an ideal of a field F, $\ker F$ must either be $\{0\}$ or F. If the kernel is the zero element, ρ must be injective. Otherwise, if $\ker \rho = F$, every element in F gets mapped to zero in R. However, a ring homomorphism always maps $1 \to 1$, so the ring must not have a unity. As R is assumed to be a commutative ring with unity, it must be the zero ring, by contradiction.

Problem 3

Let I and J be ideals of a ring R. We take the ideal sum to be $I + J = \{r + s : r \in I, s \in J\}$. Note that $I + J$ satisfies the absorbing property, because for any $r \in R$ and $k = i + j \in I + J$, the product $rk = ri + rj \in I + J$ since the first term is in I and the second is in J. That $I + J$ is an additive subgroup of R follows directly from the additive properties of I and J, so $I + J$ is an ideal in R.

In fact, every ideal K containing both I and J must contain $I + J$. In other words, for any $i \in I$ and $j \in J$, the sum $i + j$ must be in K. This follows from the fact that K must form an additive subgroup – i.e. the sum of two elements in K must be in K. As both $i, j \in K$, it is clear that $i + j \in K$, and consequently K must contain $I + J$.

Problem 4

Let I and J be ideals in a ring R. We define the ideal product to be

$$I \cdot J = \left\{ \sum_{i=1}^{n} r_i s_i : r_i \in I, s_i \in J \right\}.$$

In other words, $I \cdot J$ contains all finite sums of products of two elements, one each from I and J. We wish to show that $I \cdot J$ is an ideal contained in $I \cap J$, i.e. that every element of the ideal product is in I as well as J. First note that for all i, we know that $r_i s_i \in I$ by the absorbing property of $r_i \in I$ and that $r_i s_i \in J$ by the absorbing property of $s_i \in J$. Since both I and J are additive subgroups of R, the sum $\sum_{i=1}^{n} r_i s_i$ must also be in both I and J, and we are done.

Problem 5

Let r and n be elements of the ring $\mathbb{Z}$ and let (n) be the principal ideal generated by n. We wish to show that $r \in (n)$ if and only if n divides r. If $r \in (n)$, it can be written as $r = ns$ for some $s \in \mathbb{Z}$, by definition of the ideal (n), and thus n divides r. Conversely, if n divides r, there exists some $s \in R$ such that $r = ns$. Since (n) contains every multiple of n, $r \in (n)$, and we are done.

The ideal sum $(n) + (m)$ is the set of all sums of multiples of n or m. It contains elements such as $n, m, n + m, 2n + m, n + 2m, 2n + 2m, \cdots$. The intersection $(n) \cap (m)$ is simply the set of elements of $\mathbb{Z}$ that are divisble by both n and m. The ideal product $(n) \cdot (m)$ on the other hand, is the set of all elements that are divisible by nm. Note carefully that divisibility by nm is not necesarily equivalent to divisibility by m and n. Take, for example, the ideals (2) and (4) – the product ideal consists of all multiples of 8, whereas the intersection of the two ideals is the set of multiples of 4; these two sets are *not* the same.

Problem 6

Let S be a ring and R a subring of S. On the last problem set, we showed that if J is an ideal in S, then $I = R \cap J$ is an ideal in R. Let g be a map from R to S/J such that $g(r) = r + J$, for any $r \in R$. What is the kernel of f? It is the set of all elements $r \in R$ for which $r + J = 0 + J$: i.e. $R \cap J = I$. By the fundamental theorem for homomorphisms, then, we know that there exists an isomorphism $\phi : R/I \to \text{Im}g$. Thus there is an injective map from R/I to S/J, namely the composition of the injective inclusion map $\iota : \text{Im}g \to S/J$ with the isomorphism, $f = \iota \circ \phi : R/I \to S/J$. This map is, of course, a homomorphism, as it is the composition of an isomorphism and the inclusion homomorphism.

We now wish to show that f is surjective if and only if for every $s \in S$, there exists $r \in R$ such that $s \equiv r \mod J$, i.e. $s - r \in J$. First note that f is surjective if and only if for every $s + J \in S/J$, there exists and $r \in R$ such that $f(r + I) = r + J$ is equal to $s + J$. This, in turn, holds if and only if $(r + J) - (s + J) = 0 + J$; i.e. $s - r \in J$.

Problem 7

Let R be the subring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. Let $I = (2 + 3i)$ be the principal ideal in $\mathbb{Z}[i]$ generated by $2 + 3i$.

It should be clear that I contains $2+3i$ and $-3+2i$, as $1(2+3i) = 2+3i$ and $i(2 + 3i) = -3 + 2i$. In fact, the additive subgroup $(I, +)$ of the group $(\mathbb{Z}[i], +)$ is generated by $2 + 3i$ and $-3 + 2i$, because any $\mathbb{Z}[i]$-multiple of $2 + 3i$ can be written as a sum of multiples of $2 + 3i$ and $-3 + 2i$:

$$(a + bi)(2 + 3i) = (2 + 3i)a + (-3 + 2i)b.$$

To determine whether an arbitrary element of $\mathbb{Z}[i]$ such as $i + 5$ is in I, we can divide:

$$\frac{i+5}{2+3i} = \frac{i+5}{2+3i} \cdot \frac{2-3i}{2-3i} = 1 - i,$$

and so $i + 5 \in I$ as it can be written as the product of $2 + 3i$ and $1 - i$. Consequently, we can write $i \equiv -5 \mod I$.

Now consider the homomorphism $f : \mathbb{Z} \to \mathbb{Z}[i]/I$ such that $f(n) = n + I = n + (2 + 3i)$. To see that f is surjective, take any $n + I \in \mathbb{Z}[i]/I$.

Any m such that $m \equiv n \mod I$ will satisfy $f(m) = n + I$ simply because $f(m) = m + I = n + I$ (using the equivalence), and thus, since there exist such m's (a perfectly legitimate candidate is $n(2+3i)$), f must be surjective.

Note that for an integer such as 13 to be in the intersection $\mathbb{Z} \cap I$, it must be a $\mathbb{Z}[i]$-multiple of $2 + 3i$. Again, we can check this via division:

$$\frac{13}{2+3i} = \frac{13}{2+3i} \cdot \frac{2-3i}{2-3i} = 2 - 3i,$$

and so $13 \in \mathbb{Z} \cap I$. It turns out, in fact, that $\mathbb{Z} \cap I = 13\mathbb{Z}$. To show this, let us first show that $13\mathbb{Z} \subset \mathbb{Z} \cap I$ and then show that $\mathbb{Z} \cap I \subset 13\mathbb{Z}$. Note that the computation above, after the addition of an arbitrary integer n in the numerator, proves that every integer multiple of 13 is in $(2 + 3i)$, and so is in $\mathbb{Z} \cap I$. The converse, that every integer in I is a multiple of 13, is checked by the usual division for any $n \in \mathbb{Z}$:

$$\frac{n}{2+3i} \cdot \frac{2-3i}{2-3i} = \frac{2n-3ni}{13}.$$

Since we know $n \in I$, the above fraction must be in $\mathbb{Z}[i]$. Consequently, $2n$ and $3n$ must be (integer) divisible by 13. As 2, 3, and 13 are relatively prime, it follows that n must be divisible by 13 as well, and we are done.

Since $\mathbb{Z}$ is a subring of $\mathbb{Z}[i]$, and the f defined earlier is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}[i]$, the previous problem tells us that $\mathbb{Z}/(\mathbb{Z} \cap I) = \mathbb{Z}/13\mathbb{Z} \cong \mathbb{Z}[i]/(2+3i)$. In other words, we have reached the result that $\mathbb{Z}/13\mathbb{Z} \cong \mathbb{Z}[i]/I$. As $\mathbb{Z}/13\mathbb{Z}$ is a field, $\mathbb{Z}[i]/I$ must be a field as well, and thus I is a maximal ideal (recall that an ideal I of a ring R is maximal if and only if R/I is a field). Of course, any maximal ideal is prime, so I is a prime ideal as well.