Math 1530: Homework 4

Milan Capoor

17 October 2023

3.40

Let R be a commutative ring.

(a) *Let $c \in R$. Prove that*

$$\{cr : r \in R\}$$

is an ideal of R. As noted in Definition 3.27, it is called the principal ideal generated by c and is denoted by cR or (c).

An ideal is a subgroup under addition of R which has the property

$$ar \in I \quad \forall a \in I, r \in R$$

First, we seek to show that $cR = \{cr : r \in R\}$ a subgroup of R. Let c_1, c_2 be two elements in R. Then

$$c_1 r + c_2 r = (c_1 + c_2)r \quad \forall r \in R$$

but since R is a ring, $c_1 + c_2 \in R$ so cR is closed under addition. Further, it has an identity because $1 \in R$ so

$$1r = r \in \{cr : r \in R\}$$

Similarly, since R is a ring, it is already a subgroup under addition so every $r \in R$ has an inverse in R. Thus,

$$cr + cr^{-1} = c(r + r^{-1}) = c0 = 0$$

so every element in cR has an additive inverse. Finally, associativity is inherited from R. Thus, cR is a subgroup of R.

Now to check the absorption property, take any element $a \in cR$. Clearly, it will have the form $a = cr_1$ for some $r_1 \in R$. Now we take another element $r_2 \in R$ and consider

$$ar_2 = cr_1 r_2$$

However, since R is a ring, it is closed under multiplication so $r_1 r_2 \in R$. Denote the product $r = r_1 r_2 \in R$. Then $ar_2 = cr$. So clearly it is a member of cR. Thus, cR is an ideal of R. $\blacksquare$

(b) *More generally, let $c_1, \ldots, c_n \in R$. Prove that*

$$\{r_1 c_1 + r_2 c_2 + \ldots + r_n c_n : r_1, \ldots, r_n \in R\}$$

is an ideal of R. As noted in Example 3.29, it is called the ideal generated by $c_1, \ldots, c_n$ and is denoted by $(c_1, \ldots, c_n)$ or $c_1 R + \ldots + c_n R$

First we must show that $(c_1, \ldots, c_n)$ is an additive subgroup of R:

(a) Additive closure is trivial from definition of sum of products of elements in R

(b) Identity: $0 \in R$ so

$$0 + \sum_{i=1}^{n} r_i c_i = \sum_{i=1}^{n} r_i c_i$$

(c) Inverses: $c_1, \ldots, c_n$ are in R so they have additive inverses ($-c_1, \ldots, -c_n \in R$).

$$\sum_{i=1}^{n} r_i c_i + \sum_{i=1}^{n} r_i(-c_i) = \sum_{i=1}^{n} r_i(c_i - c_i) = 0$$

(d) Associativity comes from R

Now to show absorption, observe for $r, r_1, \ldots, r_n \in R$

$$r(\sum_{i=1}^{n} a_i r_i) = \sum_{i=1}^{n} a_i (r r_i)$$

And R is a ring so $rr_i \in R$ so

$$r(\sum_{i=1}^{n} a_i r_i) \in \{r_1 c_1 + r_2 c_2 + \ldots + r_n c_n : r_1, \ldots, r_n \in R\} \quad \blacksquare$$

3.41

Let R be a commutative ring. Prove that R is a field if and only if its only ideals are the zero ideal (0) *and the entire ring* R Suppose there is an ideal in R where $I \neq (0)$. Consider an element $a \in I, a \neq 0$. If R is a field, every (non-zero) element has an inverse so $b = a^{-1}$ exists with $b \in R$. Then, by absorption

$$ba = 1 \in I$$

Now we take any element $r \in R$ and observe that because $1 \in I$ the absorber property also gives

$$r1 = r \in I$$

therefore, $R = I$.

Now we want to show that other direction: if the only ideals are (0) and (1), then R is a field. Let R be a ring with those ideals. We pick any $a \in R, a \neq 0$ and consider $I = aR$. If $I \neq \{0\}$ then there is an element $a \in I$. Now we consider $a1 = a$ but $a \in I$ so $1 \in I$.

Then for any $r \in R$,

$$r1 = r \in I$$

so $r = a^{-1}$ exists for any a. Thus, R is a field. ■

3.43

The goal of this exercise is to prove that every ideal in $\mathbb{Z}$ is a principal ideal.

(a) *Let I be a non-zero ideal in $\mathbb{Z}$. Prove that I contains a positive integer.*

Suppose that I contains no positive integers. Since I is non-zero, that means there is a negative integer in I. Choose a negative integer in I and call it a. Then because I is an ideal, we should be able to choose any element in $r \in \mathbb{Z}$ and the product ar should be in I. Observe, however, that for any negative r, ar is a positive integer. This is a contradiction so I must contain a positive integer. ■

(b) *Let I be a non-zero ideal in $\mathbb{Z}$. Let c be the smallest positive integer in I. Prove that every element of I is a multiple of c. (Hint. Use division with remainder.)*

Suppose a is an element of I which is not a multiple of c.

By the division algorithm,

$$a = cm + r$$

for $m, r \in \mathbb{Z}$ and $0 < r < c$.

Clearly $cm \in I$ by absorption so $r = a - cm \in I$ by closure. But since $0 < r < c$, we have a contradiction of the minimality of c. Therefore, every element in I is a multiple of c. ■

(c) *Prove that every ideal in $\mathbb{Z}$ is principal.*

The zero ideal is trivially principal because its only element, 0, is obviously a multiple of 0.

By part (a), all non-zero ideals in $\mathbb{Z}$ contain a positive integer. By the ordering of the integers, they must

(a) contain only one positive integer

(b) have a smallest positive integer.

If there is only one positive integer in I, then it is clearly the smallest positive integer in I. So every non-zero ideal in $\mathbb{Z}$ has a smallest positive integer.

By part (b), every element of I is a multiple of that smallest positive integer c. Thus, every element in I can be written $cr : r \in R$ which is precisely the definition of a principal ideal. Thus, every ideal in $\mathbb{Z}$ is principal. ■

3.48

Let R be a commutative ring and let I and J be ideals of R.

(a) *Prove that the intersection $I \cap J$ is an ideal of R.*

We need to verify that the intersection is an abelian group under addition and that it has the absorption property.

To start, $I \cap J$ inherits associativity from R.

To see closure, let $x, y \in I \cap J$. Then (obviously) x and y are both members of each ideal. Clearly, $x + y \in I$ (because I is an ideal and thus an abelian group under addition) and similarly $x + y \in J$ so $x + y \in I \cap J$. Thus the intersection is closed under addition.

Identity: Because I and J are ideals, $0 \in I$ and $0 \in J$ ($0 \in R$ because it is a ring, so with $x \in I \cup J$, $0x = 0$). As the additive identity is in both ideals, $0 \in I \cap J$.

Inverse: Let $x \in I \cap J$. I and J are ideals so $x^{-1} \in I$ and $x^{-1} \in J$. Thus $x^{-1} \in I \cap J$

Absorption: Let $x \in I \cap J$ and $r \in R$. Consider rx. Since $x \in I$, $rx \in I$ but additionally $x \in J$ so $rx \in J$. Hence, $rx \in I \cap J$.

As $I \cap J$ is an abelian subgroup under addition of R and has the absorber property, it is an ideal of R. ■

(b) *Prove that the ideal sum*

$$I + J = a + b : a \in I \text{ and } b \in J$$

is an ideal of R.

(a) Associativity: comes from addition in R

(b) Closure: Let $a_1, a_2 \in I$ and $b_1, b_2 \in J$. Clearly $a_1 + b_1 \in I + J$ and $a_2 + b_2 \in I + J$. Then

$$\begin{aligned}(a_1 + b_1) + (a_2 + b_2) &= a_1 + a_2 + b_1 + b_2 \qquad \text{(commutativity)} \\ &= (a_1 + a_2) + (b_1 + b_2) \qquad \text{(associativity)} \\ &= a' + b' \in I + J \qquad (a' \in I, b' \in J \text{ by closure})\end{aligned}$$

(c) Identity: Let $a \in I$, $b \in J$. Since I and J are ideals, 0_I (the identity for I) and 0_J (the identity for J) exist. Then $0_I + 0_J \in I + J$ and

$$a + b + 0_I + 0_J = (a + 0_I) + (b + 0_J) = a + b \in I + J$$

(d) Inverse: Let $x \in I$ and $y \in J$. Because I is an ideal, $x^{-1} \in I$ exists. Similarly, $y^{-1} \in J$ exists. Then $x + y \in I + J$ and $x^{-1} + y^{-1} \in I + J$ by definition of $I + J$. Consider,

$$\begin{aligned}(x + y) + (x^{-1} + y^{-1}) &= x + x^{-1} + y + y^{-1} \qquad \text{(by commutativity)}\\ &= 0 + 0 = 0 \in I + J\end{aligned}$$

(e) Absorption: Let $a + b \in I + J$ and $r \in R$. We seek to show that $r(a + b) \in I + J$. By distributivity, $r(a + b) = ra + rb$. As $a \in I$, $ra \in I$ and $rb \in J$ so $ra + rb \in I + J$

As $I + J$ is an abelian subgroup under addition of R and has the absorber property, it is an ideal of R. ■

(c) *The ideal product of two ideals is defined to be*

$IJ = \{a_1b_1 + a_2b_2 + \ldots + a_nb_n : n \geq 1$ and $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J\}$.

Prove that IJ is an ideal of R

(a) Associativity: comes from R

(b) Closure: Let

$$\begin{gathered}\{a_1, \ldots, a_n : a_i \in I\}\\ \{b_1, \ldots, b_n : b_i \in J\}\\ \{c_1, \ldots, c_n : c_i \in I\}\\ \{d_1, \ldots, d_n : d_i \in J\}\end{gathered}$$

so $\sum_{i=1}^{n} a_ib_i, \sum_{i=1}^{n} c_id_i \in IJ$. Consider their sum:

$$\sum_{i=1}^{n} a_ib_i + \sum_{i=1}^{n} c_id_i = \sum_{i=1}^{n} a_ib_i + c_id_i$$

But since a_i and c_i are both in I for all $1 \leq i \leq n$, we can define a new sequence

$$a' = \{a_1, \ldots, a_n, c_1, \ldots, c_n\}$$

and similarly for J,

$$b' = \{b_1, \ldots, b_n, d_1, \ldots, d_n\}$$

So,

$$\sum_{i=1}^{n} a_i b_i + c_i d_i = \sum_{i=1}^{2n} a'_i b'_i \in IJ$$

(c) Identity: $0_I \in I$ and $0_J \in J$ so for an element $\sum_{i=1}^{n} a_i b_i \in IJ$, $0_I 0_J \in IJ$ (with $n = 1$) and

$$0_I 0_J + \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} a_i b_i$$

(d) Inverse: Let $\sum_{i=1}^{n} a_i b_i$ be an element in IJ. Then for each $\forall a_i \in I, \exists a_i^{-1} \in I$ and $\forall b_i \in J, \exists b_i^{-1} \in J$ because I and J are ideals. Thus, $\sum_{i=1}^{n} a_i^{-1} b_i^{-1} \in IJ$ so

$$\begin{aligned}
\sum_{i=1}^{n} a_i b_i + \sum_{i=1}^{n} a_i^{-1} b_i^{-1} &= \sum_{i=1}^{n} a_i b_i + a_i^{-1} b_i^{-1} \\
&= \sum_{i=1}^{n} a_i b_i + (b_i a_i)^{-1} \qquad \text{(by inverse properties)} \\
&= \sum_{i=1}^{n} a_i b_i + (a_i b_i)^{-1} \qquad \text{(by commutativity)} \\
&= 0
\end{aligned}$$

(e) Absorption: Let $\sum_{i=1}^{n} a_i b_i$ be an element in IJ and $r \in R$. Then

$$r\left(\sum_{i=1}^{n} a_i b_i\right) = \sum_{i=1}^{n} r a_i b_i$$

But as $a_i \in I$ and I ideal, $r a_i \in I \forall a_i$. Thus,

$$\sum_{i=1}^{n} r a_i b_i = \sum_{i=1}^{n} a'_i b_i \in IJ$$

As IJ is an abelian subgroup under addition of R and has the absorber property, it is an ideal of R. ■

(d) *One might ask why the product IJ of ideals isn't simply defined as the set of products*

$$ab : a \in I \text{ and } b \in J$$

The answer is that the set of products need not be an ideal. Here is an example. Let $R = \mathbb{Z}[x]$, and let I and J be the ideals

$$I = 2\mathbb{Z}[x] + x\mathbb{Z}[x] \text{ and } J = 3\mathbb{Z}[x] + x\mathbb{Z}[x].$$

Prove that the set of products $\{ab : a \in I \text{ and } b \in J\}$ is not an ideal.

I can also be expressed as the set of polynomials

$$a \in I = 2a_0 + \sum_{i=1}^{n} a_i x^i$$

Similarly, J is

$$b \in J = 3b_0 + \sum_{i=1}^{n} b_i x^i$$

Thus to show that the set of products of ab is not an ideal, we need to show that it is not closed under addition.

Consider $6 + x$. This is not itself a product ab of elements in I and J because if both a and b are of degree 1, then ab is of degree two. Similarly, if both a and b are of degree 0 then ab is of degree 0. Finally, assume WLOG that a is of degree 0 and b is of degree 1. Then $ab = a(b_1 + x) = ab_1 + ax \implies a = 1$ but $1 \notin I$. Hence we have a contradiction so $6 = x$ is not a product.

But

$$6 + x = 3(4 + x) - 2(3 + x) = 12 + 3x - 6 - 2x$$

and clearly $3(4 + x), -2(3 + x) \in \{ab\}$ because $3, 3 + x \in J$, and $4 + x, -2 \in I$ so we have shown that there is an element which the sum of two elements in $\{ab\}$ which is not itself in $\{ab\}$. Therefore, $\{ab\}$ is not closed under addition so it is not an ideal. ■

(e) *On the other hand, prove in general that if either I or J is a principal ideal, then the set of products $\{ab : a \in I \text{ and } b \in J\}$ is an ideal.*

Denote $I \circ J = \{ab : a \in I \text{ and } b \in J\}$

(a) Associativity: comes from R

(b) Closure: As either I or J is principal, assume WLOG it is I that is principal. Then let $a_1 = ca'_1, a_2 = ca'_2$ be any two elements in I. Further let $b_1, b_2 \in J$. Then for the arbitrary composition of two elements in $I \circ J$,

$$a_1b_1 + a_2b_2 = ca'_1b_1 + ca'_2b_2 = c(a'_1b_1 + a'_2b_2)$$

As I and J are ideals of R, $a'_1b_1 + a'_2b_2 \in R$ so $c(a'_1b_1 + a'_2b_2) \in I \circ J$

(c) Identity: As both I and J are ideals, $0 \in I \cap J$ because $0 \in R$ so $\forall a \in I : 0a \in I$ and $\forall b \in J : 0b \in J$ so both $0b = 0$ and $a0 = 0$ are in $I \circ J$. Therefore, $ab + 0 \in I \circ J$.

(d) Inverse: $\forall a \in I$, $\exists a^{-1} \in I$ and $\forall b \in J$, $\exists b^{-1} \in J$. So $a^{-1}b^{-1} \in I \circ J$. Further, by commutativity, $a^{-1}b^{-1} = b^{-1}a^{-1} = (ab)^{-1}$ so the inverse

$$ab + (ab)^{-1} = 0$$

exists in $I \circ J$ for all a, b

(e) Absorption: Let $ab \in I \circ J$, $r \in R$. By associativity $r(ab) = (ra)b$ and by $a \in I$ with I ideal, $ra \in I$ so $(ra)b \in I \circ J$

As $I \circ J$ is an abelian subgroup under addition of R and has the absorber property, it is an ideal of R. ■

3.52

(a) Let $m \neq 0$ be an integer. Prove that the ideal $m\mathbb{Z}$ is a prime ideal (and hence also a maximal ideal) if and only if $|m|$ is a prime number in the usual sense of primes in $\mathbb{Z}$.

We need to show both that $m\mathbb{Z}$ being a prime ideal implies $\left|m\right|$ is prime and that $\left|m\right|$ being prime implies $m\mathbb{Z}$ is a prime ideal.

Beginning with second statement, we observe that if $\left|m\right|$ is prime, then by Proposition 3.20 $\mathbb{Z}/m\mathbb{Z}$ is a field. By Theorem 3.43, R/I is a field if and only if I is maximal, so $m\mathbb{Z}$ is maximal. Corollary 3.44 neatly completes the proof by showing that every maximal ideal is a prime ideal.

To see the opposite direction, note that $m\mathbb{Z}$ is a prime ideal if and only if $\mathbb{Z}/m\mathbb{Z}$ is an integral domain. Thus, $\mathbb{Z}/m\mathbb{Z}$ has no zero divisors. Suppose $\left|m\right|$ is composite, i.e. $ab = m$ for some $a, b \in \mathbb{Z}$. Then

$$(a + m\mathbb{Z})(b + m\mathbb{Z}) = ab + m\mathbb{Z} = 0 + m\mathbb{Z}$$

but this is a contradiction of the fact that $\mathbb{Z}/m\mathbb{Z}$ is an integral domain. Hence, $\left|m\right|$ must be prime. ■

(b) Let F be a field, and let $a, b \in F$ with $a \neq 0$. Prove that the principal ideal $(ax + b)F[x]$ is a maximal ideal of the polynomial ring $F[x]$.

The ideal $I = (ax + b)F[x]$ is a maximal ideal of $R = F[x]$ if and only if R/I is a field. That is, with $p(x), q(x) \in F[x]$,

$$(p(x) + I)(q(x) + I) = p(x)q(x) + I = 0 + I$$

So, equivalently, we want to show that $p(x)q(x) \in (ax + b)F[x]$

But as I is principal, every element of I is divisible by $ax + b$. So we need to show that $ax + b \Big| p(x)q(x)$ for all $p, q \in F[x]$.

We are concerned with the product $p(x)q(x)$ in a ring of polynomials so the product will also be in $F[x]$. For simplicity we will let $f(x) = p(x)q(x)$. Then we apply polynomial division:

$$f(x) = (ax + b)m + r$$

where $m, r \in F[x]$ and $0 \leq \deg(r) < \deg(ax + b) = 1$. Thus we know $f(x)$ is in a constant coset $f(x) - r \in I$. So by closure, $p(x)q(x) \in I$. ■

3.54

Let R be a ring, let $b, c \in R$, and let $E_{b,c} : R[x, y] \to R$ be the evaluation homomorphism described in Exercise 3.13.

(Hint. Use Proposition 3.34 and Theorem 3.43.)

(a) If R is an integral domain, prove that $\ker(E_{b,c})$ is a prime ideal of $R[x, y]$.

By proposition 3.34b(i), the kernel of a ring homomorphism $\phi : R \to R'$ is an ideal of R, so we know that $\ker(E_{b,c})$ is an ideal of $R[x, y]$.

Now we need to show that it is prime. From Theorem 3.43a, I is a prime ideal if and only if the quotient ring R/I is an integral domain. So in this case, we need to show that $R[x, y]/\ker(E_{b,c})$ is an integral domain.

Applying 3.34b(iii), we then know there is an injective ring homomorphism from $R[x, y]/\ker(E_{b,c}) \to R$. In fact, if we can show that $E_{b,c} : R[x, y] \to R$ is surjective, then by the isomorphism theorem, the map $R[x, y]/\ker(E_{b,c}) \to R$ is actually an isomorphism.

From the definition of $E_{b,c}$,

$$E_{b,c}[f(x, y)] = f(b, c) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} b^i c^j$$

This is clearly surjective because with $a_{ij} \in R$,

$$a_{ij} = a_{ij} b^0 c^0 + \sum_{i=1}^{m} \sum_{j=1}^{n} 0 b^i c^j$$

Therefore, we have a surjective homomorphism from $R[x, y] \to R$, a homomorphism from $R[x, y] \to R/\ker(E_{b,c})$, and an isomorphism from $R[x, y]/\ker(E_{b,c}) \to R$.

Finally, if R is an integral domain and there is an isomorphism from $R[x, y]/\ker(E_{b,c})$ to R, $R[x, y]/\ker(E_{b,c})$ must also be an integral domain because isomorphic rings have the same structure. Thus from theorem 3.43, $\ker(E_{b,c})$ is a prime ideal. $\blacksquare$

(b) If R is a field, prove that $\ker(E_{b,c})$ is a maximal ideal of $R[x, y]$.

From above, we know that $\ker(E_{b,c})$ is an ideal of $R[x, y]$. And by Theorem 3.43, an ideal I is maximal if and only if the quotient ring R/I is a field.

We already showed that $R[x, y]/\ker(E_{b,c})$ is isomorphic to R so if R is a field, then $R[x, y]/\ker(E_{b,c})$ is a field so $\ker(E_{b,c})$ is maximal. ∎