MATH 436 Notes: Ideals.

Jonathan Pakianathan

December 1, 2003

1 Ideals and Subrings

Definition 1.1 (Subring). *Let $(R, +, \cdot)$ be a ring and S a subset of R which is itself a ring under $+$ and $\cdot$ with the same multiplicative identity 1 then we call S a subring of R.*

For example the integers $\mathbb{Z}$ are a subring of the rational numbers $\mathbb{Q}$.

Definition 1.2 (Ideal). *Let R be a ring.*

A left ideal I of R is a subset of R such that
(1) $(I, +)$ is a subgroup of $(R, +)$.
(2) $r \in R, \alpha \in I \implies r\alpha \in I$.

Similarly a right ideal J of R is a subset of R such that
(1) $(J, +)$ is a subgroup of $(R, +)$.
(2) $r \in R, \alpha \in J \implies \alpha r \in J$.

An ideal K of R is a subset that is both a left ideal and a right ideal of R. For emphasis, we sometimes call it a two-sided ideal but the reader should understand that unless qualified, the word ideal will always refer to a two-sided ideal.

The zero ideal (0) and the whole ring R are examples of two-sided ideals in any ring R. A (left)(right) ideal I such that $I \neq R$ is called a proper (left)(right) ideal of R.

Note in a commutative ring, left ideals are right ideals automatically and vice-versa. Also note that any type of ideal is a subring without 1 of the ring.

However the converse is not true, for example $\mathbb{Z}$ is a subring of $\mathbb{Q}$ but not an ideal.

Definition 1.3 (Ideals generated by sets). *Let R be a ring and let X be a subset of R. Then we define the left ideal generated by X to be:*

$$(X)_L = \{\sum_{i=1}^{n} s_i x_i | s_i \in R, x_i \in X, n \in \mathbb{N}\}.$$

It is easy to show that $(X)_L$ is the smallest left ideal of R that contains X.

Similarly we define the right ideal generated by X to be:

$$(X)_R = \{\sum_{i=1}^{n} x_i s_i | s_i \in R, x_i \in X, n \in \mathbb{N}\}.$$

It is easy to show that $(X)_R$ is the smallest right ideal of R that contains X.

Finally we define the ideal generated by X to be:

$$(X) = \{\sum_{i=1}^{n} r_i x_i s_i | r_i, s_i \in R, x_i \in X, n \in \mathbb{N}\}.$$

It is easy to show that (X) is the smallest two-sided ideal of R that contains X.

Of course when R is commutative, $(X)_L = (X)_R = (X)$ in general.

Definition 1.4 (Principal ideals). *Let R be a ring. Every (left)(right) ideal I is generated by a subset of R, namely I itself, however it is useful to ask if we can find a smaller generating set.*

A (left)(right) ideal I is called finitely generated if it is generated as a (left)(right) ideal by a set X with $|X| < \infty$.

A (left)(right) ideal I is called principal if it is generated as a (left)(right) ideal by a single element.

Note for principal ideals generated by a single element x we have:

$$(x)_L = \{rx | r \in R\}$$

$$(x)_R = \{xr | r \in R\}$$

and

$$(x) = \{sxr | s, r \in R\}.$$

The zero ideal (0) and the whole ring $(1) = R$ are always examples of principal ideals in any ring R.

Example 1.5 (Ideals of $\mathbb{Z}$). *Let us find the ideals of the ring $\mathbb{Z}$. Since it is commutative, there is no difference between left and right ideals.*

Let I be an ideal of $\mathbb{Z}$, in particular I is a subgroup of $(\mathbb{Z}, +)$ and so by our previous classification of such subgroups, we have $I = d\mathbb{Z}$ for some integer $d \geq 0$. Thus in particular I is a principal ideal generated by d.

Thus the ideals of $\mathbb{Z}$ are exactly $\{(d) | d \in \mathbb{N}\}$.

Definition 1.6 (Principal Ideal Rings and Domains). *An integral ring R such that every left ideal, every right ideal and every two-sided ideal is principal is called a principal ideal ring.*

An integral domain R such that every ideal is principal is called a principal ideal domain which is abbreviated as PID.

(Thus as usual domain refers to the commutative version of the concept.)

Thus by the last example, we see that $\mathbb{Z}$ is an example of a PID.

Lemma 1.7. *Let R be a ring.*
(a) If a (left)(right) ideal I of R contains a unit of R then $I = R$.
(b) In a division ring R, the only (left)(right) ideals of R are (0) and R. Thus every division ring is a principal ideal ring and every field is a PID.

Proof. Let I be a left ideal of R and suppose $u \in I$ where u is a unit of R. Since for every $r \in R, r = (ru^{-1})u$ we have that $r \in I$ for all $r \in R$ and so $I = R$. A similar proof works for right ideals. This proves part (a).

In a division ring R, every nonzero element is a unit, so any nonzero ideal will contain a unit and hence have to equal R by part (a). This proves part (b). □

Two-sided ideals play the role of normal subgroups in the theory of rings as the following construction shows:

Definition 1.8 (Quotient Rings). *Let R be a ring and let I be a two-sided ideal of R.*

We define the quotient ring R/I as follows.

Since $(R, +)$ is an Abelian group, $(I, +)$ will be a normal subgroup and so $R/I = \{r + I | r \in R\}$ will inherit the structure of an Abelian group with well-defined addition:

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I.$$

We define a multiplication as follows:

$$(r_1 + I)(r_2 + I) = (r_1 r_2 + I)$$

for all $r_1, r_2 \in R$*.*

To show it is well-defined assume $r_1+I = r_1'+I$ *and* $r_2+I = r_2'+I$*. Then* $r_1 = r_1'+\alpha$ *and* $r_2 = r_2'+\beta$ *where* $\alpha, \beta \in I$*. Then* $r_1r_2 = r_1'r_2'+(\alpha r_2'+r_1'\beta+\alpha\beta)$*. The term in brackets is in* I *since* I *is a two-sided ideal of* R*. Thus indeed* $r_1r_2 + I = r_1'r_2' + I$ *and the multiplication is well-defined.*

Once we know it is well-defined, the properties of a ring are automatically inherited from R*. Thus* R/I *is a ring with multiplicative identity* $1 + I$ *and additive identity* $0 + I = I$*.*

It then follows that the quotient map $\phi : R \to R/I$ *given by* $\phi(r) = r + I$ *for all* $r \in R$ *is an epimorphism of rings.*

Quite often the notation $\overline{r}$ *is used instead of* $r + I$ *for elements of* R/I*. Thus* $\overline{r}\ \overline{s} = \overline{rs}$*,* $\overline{r} + \overline{s} = \overline{r+s}$ *and* $\overline{r} = \overline{s}$ *if and only if* $r = s + \alpha$ *for some* $\alpha \in I$*. So in particular* $\overline{r} = \overline{0}$ *if and only if* $r \in I$*.*

Sometimes one also writes $r \equiv s \bmod I$ *when* $\overline{r} = \overline{s}$*.*

Example 1.9. *Since* (n) *is an ideal of* $\mathbb{Z}$ *we may form the quotient ring* $\mathbb{Z}/(n)$*. This is the ring of integers modulo* n *which we have worked with often in the past. We will continue to use the notation* $\mathbb{Z}/n\mathbb{Z}$ *for this ring.*

For any ring R*,* $R/(0) \cong R$ *and* R/R *is the zero ring.*

Proposition 1.10 (Kernels and Images of homomorphisms). *Let* $f : R_1 \to R_2$ *be a homomorphism of rings. We define*

$$Ker(f) = \{r \in R_1 | f(r) = 0\}.$$

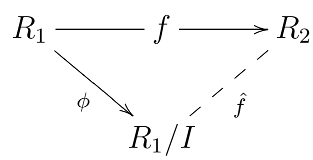
Then $Ker(f)$ *is a two-sided ideal of* R_1 *and* $Im(f)$ *is a subring of* R_2*.*

Proof. $Ker(f)$ is a subgroup of $(R_1, +)$ from group theory. If $r \in R_1$ and $\alpha \in Ker(f)$ then $f(r\alpha) = f(r)f(\alpha) = f(r)0 = 0$ and so $r\alpha \in Ker(f)$. Similarly, $\alpha r \in Ker(f)$ and so $Ker(f)$ is a two-sided ideal of R_1.

To show $Im(f)$ is a subring of R_2 is a simple exercise left to the reader. □

The basic factorization lemma for homomorphisms, also holds in the category of rings:

Theorem 1.11 (Factorization of homomorphisms). *Let R_1 and R_2 be rings and I a two-sided ideal of R_1. Let $f : R_1 \to R_2$ be a homomorphism of rings. There is a homomorphism $\hat{f}$ of rings making the following diagram commute*



if and only if $I \subseteq Ker(f)$. In this case, $Ker(\hat{f}) = Ker(f)/I$ and $\hat{f}(r+I) = f(r)$ for all $r \in R_1$.

Proof. Considering the similar factorization theorem in the category of groups, we see that the existance of $\hat{f}$ implies $I \subseteq Ker(f)$ and conversely if $I \subseteq Ker(f)$, there is a homomorphism $\hat{f}$ **of additive groups** making the diagram commute given by the stated formula and with the stated kernel.

It only remains to check that $\hat{f}$ is in fact a homomorphism of rings.

$\hat{f}(1+I) = f(1) = 1$ and $\hat{f}((r+I)(s+I)) = \hat{f}(rs+I) = f(rs) = f(r)f(s) = \hat{f}(r+I)\hat{f}(s+I)$ and so this is indeed the case. This completes the proof. ☐

This factorization theorem yields the fundamental first isomorphism theorem in the category of rings:

Theorem 1.12 (First Isomorphism Theorem). *Let $f : R_1 \to R_2$ be a homomorphism of rings. Then f induces an isomorphism*

$$R_1/Ker(f) \cong Im(f).$$

Proof. Apply the factorization theorem to the case $I = Ker(f)$. Then $\hat{f}$ has trivial kernel $Ker(f)/Ker(f)$ and hence is a monomorphism of rings $R_1/I \to R_2$.

Since $\hat{f}$ and f have the same images, $\hat{f}$ then gives an isomorphism between R_1/I and $Im(f)$. ☐

2 Ideals in a matrix ring

We will now look at an example that will illustrate the difference between left ideals, right ideals and two-sided ideals.

Let D be a division ring, e.g. a field. Consider the ring $R = Mat_n(D)$.

For every $1 \leq i, j \leq n$, let $\mathbb{T}^{ij} \in R$ be the matrix whose (i, j)-entry is 1 but whose other entries are zero.

Then given any $\mathbb{B} \in Mat_n(R)$, a simple computation shows $\mathbb{T}^{ij}\mathbb{B}$ is a matrix whose ith row is the jth row of $\mathbb{B}$ and whose other rows are zero.

In other words if we denote the (m, n)-entry of $\mathbb{B}$ by b_{mn} we have

$$\mathbb{T}^{ij}\mathbb{B} = \sum_{k=1}^{n} b_{jk}\mathbb{T}^{ik}.$$

It follows from this that the right ideal generated by $\mathbb{T}^{ij}$ is given by the matrices which have zero entries outside the ith row, i.e.,

$$(\mathbb{T}^{ij})_R = \{\mathbb{A} | a_{mn} = 0 \text{ when } m \neq i\}.$$

It is easy to check that for $n > 1$, these are examples of right ideals of R which are not left ideals.

Similarly given any $\mathbb{A} \in Mat_n(R)$, a simple computation shows that $\mathbb{A}\mathbb{T}^{ij}$ is a matrix whose jth column is the ith column of $\mathbb{A}$ but whose other columns are zero. In other words we have:

$$\mathbb{A}\mathbb{T}^{ij} = \sum_{k=1}^{n} a_{ki}\mathbb{T}^{kj}.$$

It follows that the left ideal generated by $\mathbb{T}^{ij}$ is given by the matrices which have zero entries outside the jth column, i.e.,

$$(T^{ij})_L = \{\mathbb{B} | b_{mn} = 0 \text{ when } n \neq j\}.$$

It is easy to check that for $n > 1$, these are examples of left ideals of R which are not right ideals.

Now suppose that J is a nonzero two-sided ideal of R. Take a nonzero matrix $\mathbb{B} \in J$, thus $b_{ms} \neq 0$ for some $1 \leq m, s \leq n$.

By our previous computations, it follows that $\mathbb{T}^{im}\mathbb{B}\mathbb{T}^{sj} = b_{ms}\mathbb{T}^{ij}$ for all $1 \leq i, j \leq n$. Since D is a division ring, b_{ms} is a unit in D and so we may multiply both sides with $b_{ms}^{-1}\mathbb{I}$ and conclude that $\mathbb{T}^{ij}$ is in the ideal J (since $\mathbb{B} \in J$) for all $1 \leq i, j \leq n$.

Since we have $\mathbb{A} = \sum_{i,j=1}^{n} a_{ij}\mathbb{T}^{ij}$ for all $\mathbb{A} \in R$ it follows that $\mathbb{A} \in J$ for all $\mathbb{A} \in R$ and so $J = R$.

Thus we see that R has no two-sided ideals besides (0) and R itself.

So notice there is a big difference between left ideals, right ideals and two-sided ideals of $Mat_n(D)$ when $n > 1$.

Definition 2.1. *A ring R is called simple if it has no nonzero proper two-sided ideals.*

Thus a simple ring R has no quotient rings besides itself and the zero ring.

Every division ring D is simple as it has no nonzero proper ideals of any sort.

If D is a division ring, then $Mat_n(D)$ is a simple ring but is not a division ring when $n > 1$ as some nonzero elements are not units (hence it contains proper nonzero left (right) ideals) as we have seen.