1-18-1994

Ideals.

A subgroup of a group is a subset of the group which is a group in its own right, under the induced operations. There is an analogous definition for **subrings**.

Definition. Let R be a ring. A **subring** is a subset $S \subset R$ such that:

1. S is a subgroup of the additive group $(R, +)$.

2. S is closed under multiplication: If $s, t \in S$, then $st \in S$.

   If R is a ring with unity, the following condition is *often* assumed:

3. The multiplicative identity of R is contained in S: i.e. $1 \in S$.

("Often" means that you ought to ascertain by reading the source whether the author intends this or not.)

The important "subobjects" in ring theory are **ideals**, which are analogous to normal subgroups of groups.

Definition. Let R be a ring. A **left ideal** I of R is a subset $I \subset R$ such that:

1. I is a subgroup of the additive group $(R, +)$.

2. If $r \in R$ and $x \in I$, then $rx \in I$. In other words, I is closed under *left* multiplication by arbitrary ring elements.

   Likewise, A **right ideal** I of R is a subset $I \subset R$ such that:

1. I is a subgroup of the additive group $(R, +)$.

2. If $r \in R$ and $x \in I$, then $xr \in I$. In other words, I is closed under *right* multiplication by arbitrary ring elements.

   If I is both a left ideal and a right ideal, I is a **two-sided ideal**.

If R is commutative, there is obviously no difference between left ideals, right ideals, and two-sided ideals.

In the course of attempting to prove Fermat's Last Theorem, mathematicians were led to introduce rings in which **unique factorization** failed — that is, it might be possible to factor a ring element into "primes" in more than one way. In an attempt to restore unique factorization, they were led to introduce "ideal numbers" (= ideals). Ideals also arise in a natural way when one attempts to form **quotient rings**.

Examples.

1. In any ring R, R and $\{0\}$ are ideals. A **proper ideal** is an ideal other than R; a **nontrivial ideal** is an ideal other than $\{0\}$. $\square$

2. Let I be an ideal in a ring with 1. If $1 \in I$, then $I = R$.

   Indeed, if $r \in R$, then $r = r \cdot 1 \in I$, so $R \subset I$, and $R = I$. $\square$

3. (Constructions)

   a. The intersection of a family of (left, right, two-sided) ideals is a (left, right, two-sided) ideal.

b. If $\{I_1, \ldots, I_n\}$ is a family of (left, right, two-sided) ideals, the **ideal sum**

$$\sum_{k=1}^{n} I_k = \{x_1 + \cdots + x_n \mid x_k \in I_k\}$$

is a (left, right, two-sided) ideal.

c. If I and J are (left, right, two-sided) ideals, the **ideal product**

$$IJ = \{x_1 y_1 + \cdots + x_n y_n \mid x_i \in I, y_i \in J\}$$

is a (left, right, two-sided) ideal. (Thus, IJ consists of all finite sums of products xy, $x \in I$, $y \in J$.)

I'll prove the first statement by way of example. Let $\{I_a\}$ be a family of left ideals, and let $I = \cap_a I_a$. Since $0 \in I_a$ for all a, $0 \in I$, and I is certainly nonempty. Let $x, y \in I$. Then $x, y \in I_a$ for all a, so $x - y \in I_a$ for all a, and hence $x - y \in I$. This proves that I is a subgroup.

If $r \in R$ and $x \in I$, then $x \in I_a$ for all a, so $rx \in I_a$ for all a (since I_a is a left ideal). Therefore, $rx \in I$, and I is a left ideal.

The proof for right ideals is symmetric, and the proof for two-sided ideals follows from the left and right cases. □

4. In $\mathbb{Z}$, the ideals are exactly the subsets $n\mathbb{Z} = \langle n \rangle$.

First, if I is an ideal in $\mathbb{Z}$, then I is a subgroup of $(\mathbb{Z}, +)$, so $I = n\mathbb{Z}$ for some n. ("Subgroups of cyclic groups are cyclic.")

Conversely, let $n \in \mathbb{Z}$. $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. I claim that it's an ideal. Let $nk \in n\mathbb{Z}$ and let $m \in \mathbb{Z}$. Then $m \cdot (nk) = n \cdot (mk) \in n\mathbb{Z}$, so $m\mathbb{Z}$ is closed under multiplication by arbitrary ring elements. Hence, it's an ideal. □

5. If F is a field, the only ideals are $\{0\}$ and F.

Let I be an ideal. Assume $I \neq \{0\}$, and find $x \neq 0$ in I. Since F is a field, x is invertible; since I is an ideal, $1 = x^{-1} \cdot x \in I$. Therefore, $I = F$. □

Definition. If R is a ring, the (left) **principal ideal generated by** a is

$$Ra = \{ra \mid r \in R\}.$$

The (two-sided) **principal ideal generated by** a is

$$RaR = \{ras \mid r, s \in R\}.$$

Principal ideals will most often arise in the context of commutative rings. In this case, $Ra = RaR = aR$, and I'll often denote the principal ideal generated by a by $\langle a \rangle$.

To see that Ra is indeed a left ideal, note that it is obviously nonempty (e.g. $0 \cdot a = 0 \in Ra$). If $ra, sa \in Ra$, then $ra - sa = (r - s)a \in Ra$, so Ra is a subgroup of the additive group of R. Finally, if $ra \in Ra$ and $s \in R$, then $s \cdot (ra) = (rs) \cdot a \in Ra$. Hence, Ra is a left ideal. The proof that RaR is a two-sided ideal is similar, and is left as an exercise.

With this terminology, the previous example shows that every ideal in $\mathbb{Z}$ is principal.

Definition. An integral domain in which every ideal is principal is a **principal ideal domain** (often abbreviated to **PID**).

Fields are trivially PIDs, since the only ideals are $\{0\}$ and $F = \langle 1 \rangle$. A more interesting class of examples: If F is a field, the polynomial ring $F[x]$ is a PID.

More generally, suppose S is a subset of a ring R. Let I be the intersection of all (left, right, two-sided) ideals containing S. Since R is an ideal containing S, the intersection is nontrivial; it is nonempty, since it contains S. I is an ideal, by the remarks above, and it is plainly the smallest (left, right, two-sided) ideal containing S. I is **the ideal generated by** S; write $I = \langle S \rangle$.

For example, if $S = \{x_1, \ldots, x_n\}$, then $\langle x_1, \ldots, x_n\rangle$ denotes the ideal generated by the x_i. This notation is consistent with the notation $\langle x\rangle$ for the principal ideal generated by x. Indeed, in terms of ideal sums,

$$\langle x_1, \ldots, x_n\rangle = Rx_1 + \cdots + Rx_n.$$

Now I'll explain why ideals are "natural" objects to study when one is looking at rings. Normal subgroups were introduced in order to construct quotient groups. The point was that normality makes coset multiplication well-defined.

Lemma. If I is a two-sided ideal in a ring R, then R/I has the structure of a ring under coset addition and multiplication. Conversely, if I is a subgroup of $(R, +)$ and coset multiplication in R/I is well-defined, then I is a two-sided ideal.

Proof. Suppose that I is a two-sided ideal in R. I is a normal subgroup of the abelian group $(R, +)$, so R/I is an abelian group. A typical coset has the form $r + I$, where $r \in R$. The operation is addition of coset representatives:

$$(r + I) + (s + I) = (r + s) + I.$$

I need to show that coset multiplication is well-defined:

$$(r + I)(s + I) = rs + I.$$

To that end, suppose that

$$r + I = r' + I, \quad \text{so} \quad r = r' + x,\ x \in I$$

$$s + I = s' + I, \quad \text{so} \quad s = s' + y,\ y \in I$$

Then

$$(r + I)(s + I) = rs + I = (r' + x)(s' + y) + I = r's' + r'y + xs' + xy + I = r's' + I = (r' + I)(s' + I).$$

Verification of the ring axioms is essentially trivial: it reduces to the axioms for R.

Now suppose that I is a subgroup of $(R, +)$, and suppose that coset multiplication $(r+I)(s+I) = rs+I$ is well-defined.

Let $s = 0$; then

$$(r + I)I = I, \quad rI + I^2 = I, \quad rI \subset I.$$

Likewise, set $r = 0$; then

$$I(s + I) = I, \quad Is + I^2 = I, \quad Is \subset I.$$

Therefore, I is a two-sided ideal. □

Definition. Let R and S be rings. A **ring homomorphism** (or a **ring map** for short) is a function $f : R \to S$ such that:

1. For all $r_1, r_2 \in R$, $f(r_1 + r_2) = f(r_1) + f(r_2)$.
2. For all $r_1, r_2 \in R$, $f(r_1 r_2) = f(r_1)f(r_2)$.

Many authors will also require that if R and S are rings with 1, then

3. $f(1_R) = 1_S$.

This is automatic in some cases; if there is any question, you should read carefully to find out what convention an author is using.

The first two properties stipulate that f should "preserve" the ring structure — addition and multiplication.

Examples.

1. The identity map $\mathrm{id} : R \to R$ is always a ring map. So is the zero map $0 : R \to R$ which maps everything to 0 (provided that 1 is not required to map to 1). $\Box$

2. Let R be a ring, I a two-sided ideal. Define $\pi : R \to R/I$ by $\pi(r) = r + I$. π is the canonical quotient map, and regarding R and R/I as additive groups, it is a group homomorphism:

$$\pi(r + s) = (r + s) + I = (s + I) + (s + I) = \pi(r) + \pi(s).$$

π is also multiplicative:

$$\pi(rs) = rs + I = (r + I)(s + I) = \pi(r)\pi(s).$$

Therefore, π is a ring map. Note that if R has a multiplicative identity 1, then $1 + I$ is an identity for R/I, and $\pi(1) = 1 + I$. $\Box$

3. What are the ring maps from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{16}$?

A ring map $f : \mathbb{Z}_{12} \to \mathbb{Z}_{16}$ is a group homomorphism of the additive groups. As such, it is determined by where 1 goes. Now $f(1)$ must have order dividing 12, because $12 \cdot f(1) = f(12) = f(0) = 0$. So the order of $f(1)$ can be 1, 2, 3, 4, 6, or 12. But $f(1)$ is an element of $\mathbb{Z}_{16}$, so its order must divide 16 — it can be 1, 2, 4, 8, or 16.

Comparing the two lists, I now know the order of $f(1)$ can be 1, 2, or 4. The elements of these orders are 0, 8, and 4. Thus, $f(1) = 0$, $f(1) = 8$, or $f(1) = 4$. The corresponding maps are $f(x) = 0$, $f(x) = 8x \bmod 16$, and $f(x) = 4x \bmod 16$.

Now I must check that these maps are actually ring maps. Since I already have additivity, it remains to check that $f(x, y) = f(x)f(y)$.

For the zero map $f(x) = 0$, this is obvious.

For $f(x) = 8x \bmod 16$, it fails:

$$f(1 \cdot 1) = f(1) = 8, \quad \text{but} \quad f(1) \cdot f(1) = 8 \cdot 8 = 0.$$

For $f(x) = 4x \bmod 16$, it fails:

$$f(1 \cdot 1) = f(1) = 4, \quad \text{but} \quad f(1) \cdot f(1) = 4 \cdot 4 = 0.$$

Hence, the only ring map $\mathbb{Z}_{12} \to \mathbb{Z}_{16}$ is the zero map. And if ring maps are required to take 1 to 1, there are no ring maps $\mathbb{Z}_{12} \to \mathbb{Z}_{16}$. $\Box$

4. Suppose $f : R \to S$ is surjective, R is a ring with 1, and $S \neq \{0\}$. Then $f(1)$ is the multiplicative identity of S.

Let $s \in S$. Since f is onto, $s = f(r)$ for some $r \in R$. Then

$$s \cdot f(1) = f(r) \cdot f(1) = f(r \cdot 1) = f(r) = s.$$

Likewise, $f(1) \cdot s = s$.

The stipulation that $S \neq \{0\}$ is to avoid the case of a ring where $1 = 0$ (in which case the ring is simply the zero ring $\{0\}$). $\Box$

Recall that normal subgroups are exactly the kernels of group homomorphisms.

Definition. The **kernel** of a ring map $\phi : R \to S$ is

$$\ker \phi = \{r \in R \mid \phi(r) = 0\}.$$

The **image** of a ring map $\phi : R \to S$ is

$$\operatorname{im} \phi = \{\phi(r) \mid r \in R\}.$$

Lemma. The kernel of a ring map is a two-sided ideal. Conversely, every two-sided ideal is the kernel of a ring map.

Proof. Let $\phi : R \to S$ be a ring map. Then $\ker \phi$ is a subgroup of $(R, +)$. Let $x \in \ker \phi$ and let $r \in R$.

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0 = 0$$

$$\phi(xr) = \phi(x)\phi(r) = 0 \cdot \phi(r) = 0$$

It follows that $rx, xr \in \ker \phi$. Hence, $\ker \phi$ is a two-sided ideal.

If I is a two-sided ideal in R, then R/I is a ring. Now the kernel of $\pi : R \to R/I$ considered as a map of abelian groups is I. The kernel of the map considered as a ring map is the same, so $\ker \pi = I$. Thus, every ideal is the kernel of a ring map. □

The last result explains the importance of ideals in ring theory. They (as opposed to subrings) are the natural "subobjects" that arise in forming quotient rings or studying ring homomorphisms.

Lemma. Let $\phi : R \to S$ be a ring map. Then $\operatorname{im} \phi$ is a subring of S.

Proof. First, $\operatorname{im} \phi$ is a subgroup of $(S, +)$.

Let $\phi(r_1), \phi(r_2) \in \operatorname{im} \phi$, where $r_1, r_2 \in R$. Then $\phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \operatorname{im} \phi$. Hence,$\operatorname{im} \phi$ is closed under multiplication.

Finally, note that if R has 1, then since $\phi(1) = 1$, $1_S \in \operatorname{im} \phi$. So if rings and subrings are required to have 1, $\operatorname{im} \phi$ is a subring in this extended sense. □

The following results are analogous to the corresponding results for groups.

Theorem. (Universal Property of the Quotient) Let $\phi : R \to S$ be a ring map, and let $I \subset \ker \phi$. There is a unique ring map $\tilde{\phi} : R/I \to S$ such that the following diagram commutes:

$$\begin{tikzcd} R \arrow[d, "\pi"'] \arrow[dr, "\phi"] & \\ R/I \arrow[r, "\tilde{\phi}"'] & S \end{tikzcd}$$

Proof. Since R, R/I, and S are abelian groups and the ring maps are maps of abelian groups, there is a unique map $\tilde{\phi}$ by the Universal Property of the Quotient for groups.

Thus, I only need to verify that $\tilde{\phi}$ is a ring map, and for that, I only need to check multiplicativity. Now $\tilde{\phi}(r + I) = \phi(r)$, by commutativity, so

$$\tilde{\phi}\left((r + I)(r' + I)\right) = \tilde{\phi}(rr' + I) = \phi(rr') = \phi(r)\phi(r') = \tilde{\phi}(r + I)\tilde{\phi}(r' + I). \ □$$

Theorem. (The First Isomorphism Theorem) Let $\phi : R \to S$ be a ring map. There is an isomorphism $\tilde{\phi} : R/(\ker \phi) \to \operatorname{im} \phi$ such that the following diagram commutes:

$$\begin{tikzcd} R \arrow[d, "\pi"'] \arrow[dr, "\phi"] & \\ R/(\ker \phi) \arrow[r, "\tilde{\phi}"'] & \operatorname{im} \phi \subset S \end{tikzcd}$$

Proof. The isomorphism $\tilde{\phi}$ exists and makes the diagram commute on the level of groups and group homomorphisms, by the First Isomorphism Theorem for Groups. Moreover, $\tilde{\phi}$ is produced via the Universal Property of the Quotient, so it is a ring map by the previous result. □

Example. Consider the ring $\mathbb{R}[x]$ and the ideal $\langle x-1 \rangle$.

There is a ring map $\phi : \mathbb{R}[x] \to \mathbb{R}$ given by

$$\phi(f) = f(1).$$

That is, ϕ evaluates the polynomial f at 1. It is routine to verify that ϕ is a ring map. Moreover, $\phi(a) = a$ for all $a \in \mathbb{R}$, so ϕ is surjective.

Obviously $\langle x-1 \rangle \subset \ker \phi$. Conversely, suppose $\phi(f) = f(1) = 0$. Write $f(x) = \sum_{k=0}^{n} a_k x^k$. Then

$$0 = f(i) = \sum_{k=0}^{n} a_k 1^k = \sum_{k=0}^{n} a_k.$$

Therefore, $a_0 = -\sum_{k=1}^{n} a_k$, and

$$f(x) = \sum_{k=1}^{n} a_k x^k - \sum_{k=1}^{n} a_k = \sum_{k=1}^{n} a_k (x^k - 1).$$

But $(x-1) \mid (x^k - 1)$ for all $k \geq 1$, so $(x-1) \mid f(x)$. Therefore, $f \in \langle x-1 \rangle$, and $\ker \phi \subset \langle x-1 \rangle$.

Since $\langle x-1 \rangle = \ker \phi$, the First Isomorphism Theorem gives

$$\frac{\mathbb{R}[x]}{\langle x-1 \rangle} = \frac{\mathbb{R}[x]}{\ker \phi} \approx \operatorname{im} \phi = \mathbb{R}. \ \square$$

©1993 by Bruce Ikenaga