11-30-1993

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 $\{0\}$. □

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 $R = I$. □

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,

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

©1993 by Bruce Ikenaga