Principal ideal domains

Last lecture we introduced the notion of a *principal ideal* in a commutative ring. These are ideals in a commutative ring R that take the form

$$(a) = aR = \{ar : r \in R\}$$

A *principal ideal domain* (PID) is an integral domain R (a commutative ring such that $ab = 0$ implies $a = 0$ or $b = 0$) such that every ideal in R is principal.

The ring of integers $\mathbb{Z}$ is the most basic example of a PID. The ideals in $\mathbb{Z}$ are

$$(0), \quad (1), \quad (2), \quad (3), \quad (4), \quad \ldots$$

PIDS are an important class of rings because they occur frequently and the theory of PIDS is considerably simpler than that of general (commutative) rings.

▸ **Let R be a non-zero commutative ring. The following are equivalent:**

(i) R is a field.

(ii) The only ideals in R are $(0) = \{0\}$ and $(1) = R$.

(iii) Every homomorphism $\phi : R \to R'$ where $R' \neq \{0\}$ is 1-1.

Proof. We show (i) implies (ii). Assume (i), i.e. R is a division ring. Consider an ideal $I \subset R$ with $I \neq (0)$. Choose $a \in I$, $a \neq 0$. Since R is a division ring, $a^{-1} \in R$. Then $1 = a^{-1}a \in I$ as $a^{-1} \in R$ and $a \in I$. Now for any $b \in R$, we have $b = b1 \in I$ as $b \in R$ and $1 \in I$. Thus (ii) holds.

Next, we show (ii) implies (iii). Assume (ii): the only ideals in R are $\{0\}$ and R. Consider a homomorphism $\phi : R \to R'$ where $R' \neq \{0\}$. Then $\ker(\phi) \subset R$ is a proper ideal as $1 \notin \ker(\phi)$. By our assumption it must be $\{0\}$. This is equivalent to ϕ being 1-1. Thus (iii) holds.

Finally, we show (iii) implies (i). Assume (iii), i.e. every homomorphism $\phi : R \to R'$ where $R' \neq \{0\}$ is 1-1. Now take $a \in R$ with $a \neq 0$. Consider the natural homomorphism $\phi : R \to R/(a)$. Suppose $R/(a) \neq \{0\}$, so that ϕ is 1-1. Then $\ker(\phi) = (0)$. On the other hand, $\ker(\phi) = (a)$. Then $(a) = (0)$ implies $a = 0$, a contradiction. Thus $R/(a) = \{0\}$, impying $(a) = R = (1)$. In particular, $1 = ar$ for some $r \in R$, so a has a multiplicative inverse. We have shown that every non-zero $a \in R$ is invertible, and thus R is a field. □

A corollary of this result is the following:

▸ **If R is a field, then R is a PID.**

This holds simply because the only ideals in a field R are the ideals $(0) = \{0\}$ and $(1) = R$ which are principal ideals.

Thus the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all examples of PIDs.

A more exotic example of a PID is the ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : \ a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

We will show this is a PID later.

We saw last lecture that the ring $\mathbb{Z}[\sqrt{-3}]$ is *not* a PID, because we showed that the ideal consisting of $a + b\sqrt{-3}$ with $a \equiv b \pmod 2$ is not principal.

Polynomial rings

Another important example involves the following construction. Let R be any ring. Define

$$R[x] = \{\text{polynomials in } x \text{ with coefficients in } R\}$$

That is, a typical element in $R[x]$ is an expression of the form

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$$

where n is a non-negative integer and $a_0, \ldots, a_n$ are elements of the ring R. The sum $f(x) + g(x)$ and product $f(x)g(x)$ of two such polynomials are defined in the usual fashion, and this makes $R[x]$ into a ring. If R is commutative, so is $R[x]$. Also, if R is an integral domain, so too is the polynomial ring $R[x]$.

▶ **If R is a field, then $R[x]$ is a PID.**

Before explaining the proof, let's explore the consequences of this result.

The rings $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ are all PIDS. This means, for example, that for any ideal $I \subset \mathbb{Q}[x]$ there exists a polynomial $f(x)$ with rational coefficients such that $I = (f(x))$. The polynomial $f(x)$ is unique up to multiplication by an element in $\mathbb{Q}^\times$.

Let p be a prime. Then $\mathbb{Z}_p$ is a field, so $\mathbb{Z}_p[x]$ is a PID. For example, consider $\mathbb{Z}_2[x]$, polynomials with coefficients in $\mathbb{Z}_2$. Some elements in this ring are

$$0, \quad 1, \quad x, \quad 1 + x, \quad x^2, \quad 1 + x^2, \quad 1 + x + x^2, \quad \ldots$$

For any ideal $I \subset \mathbb{Z}_2[x]$ we can find some such element $f(x)$ such that $I = (f(x))$.

The condition that R be a field in the result is necessary. For example, consider $\mathbb{Z}[x]$. Of course $\mathbb{Z}$ is not a field, so the result does not apply here. In fact $\mathbb{Z}[x]$ is not a PID: the ideal

$$I = \{2f(x) + xg(x) : \ f(x), g(x) \in \mathbb{Z}[x]\} \subset \mathbb{Z}[x]$$

is not a principal ideal, as you can verify.

Now let us prove the statement. We will need the following:

▶ **(Division algorithm for polynomials) Let R be a field. Consider polynomials $f(x)$ and $g(x) \neq 0$ in $R[x]$. Then there exist unique $q(x), r(x) \in R[x]$ such that**

$$f(x) = g(x)q(x) + r(x)$$

and where either $\mathbf{deg}(r(x)) < \mathbf{deg}(g(x))$ or $r(x) = 0$.

Here the degree of $f(x) = \sum a_i x^i \in R[x]$ is the largest n such that $a_n \neq 0$. We omit the proof of the division algorithm and now show that if R is a field then $R[x]$ is a PID.

Let $I \subset R[x]$ be an ideal. We must show I is principal. If $I = \{0\}$ then it is the principal ideal (0), so assume $I \neq (0)$. Let $g(x) \in I$ be non-zero and of minimal possible degree among all non-zero polynomials in I. Note $(g(x)) \subset I$. Now consider any other element $f(x) \in I$. Then the division algorithm gives us $q(x), r(x) \in R[x]$ satisyfing

$$f(x) = g(x)q(x) + r(x)$$

and $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$. Suppose $r(x) \neq 0$. Then

$$r(x) = f(x) - g(x)q(x)$$

is in I, because $f(x), g(x) \in I$ and $q(x) \in R[x]$. Furthermore, $\deg(r(x)) < \deg(g(x))$. But this contradicts our assumption that $g(x)$ has the minimal possible degree among non-zero polynomials in I. So we must have $r(x) = 0$. Then

$$f(x) = q(x)q(x)$$

This shows $f(x) \in (g(x))$. Thus $I = (g(x))$, and I is a principal ideal. This completes the proof that all ideals in $R[x]$ are principal.

Finally, we remark that if you continue to add variables to your ring, and consider polynomials in several variables, you will not get a PID. For example, consider

$$\mathbb{Q}[x][y] = \mathbb{Q}[x, y] = \{\text{polynomials in } x, y \text{ with coefficients in } \mathbb{Q}\}$$

Then the ideal generated by the polynomials x and y, which is given by $I = \{xf(x, y) + yg(x, y) : f(x, y), g(x, y) \in \mathbb{Q}[x]\}$, is not a principal ideal in $\mathbb{Q}[x, y]$.