Abstract Algebra, Lecture 11

Ideals in commutative, unitary rings

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Linköping, fall 2019

Lecture notes availabe at course homepage
http://courses.mai.liu.se/GU/TATA55/

Summary

Summary

Summary

Throughout this lecture, R, S will denote commutative, unitary rings, and I, J will denote ideals.

Definition

If $a \in R$ then $(a) = aR = \{ ar | r \in R \}$ is the *principal ideal* generated by a. The ring R is a principal ideal ring if all ideals in it are principal.

Theorem

The ring $\mathbb{Z}$ is a PID.

Proof.

All ideals are also additive subgroups; for Z, those subgroups are $n\mathbb{Z}$. □

Theorem

Any quotient of a PID is a PID.

Proof.

If L is an ideal of R/I, then, by the correspondence theorem, $L = J/I$ for some ideal $J \supseteq I$. This ideal is of the form $J = (b)$ since R is a PID. Take a coset $c + I \in J/I \subset R/I$. Then $c \in J$, so $c = rb$ for some $r \in R$, hence $c + I = rb + I = rb + rI = r(b + I)$. This shows that $L = (b + I)$. □

Example

The ring $\mathbb{Z}_{12} = \frac{\mathbb{Z}}{12\mathbb{Z}}$ is a PID. The ideal $L = \{[0]_{12}, [4]_{12}, [8]_{12}\}$ lifts to $4\mathbb{Z} \supset 12\mathbb{Z}$. We have that $4\mathbb{Z} = (4)$. Consequently, $L = ([4]_{12})$.

Theorem

The polynomial ring $\mathbb{Z}[x]$ is not a PID.

Proof.

Let $I = (2, x) = \{ 2f(x) + xg(x) | f(x), g(x) \in \mathbb{Z}[x] \}$. Suppose, towards a contradiction, that $I = (h(x))$.
Since $2 \in I$, $2 = a(x)h(x)$. So $h(x)$ is a constant, say $h(x) = h$.
Since $x \in I$, $x = b(x)h$. So $b(x) = cx + d$, and in fact $d = 0$, $c = \pm 1$, $h = \pm 1$. But then $(h(x)) = \mathbb{Z}[x]$, a contradiction. □

Definition

I is a *prime ideal* if

$$xy \in I \implies x \in I \text{ or } y \in I.$$

Lemma

(0) is a prime ideal iff R is a domain.

Proof.

If $xy = 0$ but $x, y \neq 0$ then x is a non-zero zero-divisor, and R is not a domain.
If R is not a domain, it has a non-zero zero-divisor x, so that $xy = 0$ for $y \neq 0$, thus (0) is not prime. □

Theorem

In $\mathbb{Z}$, the zero ideal is prime, as is (p) with p prime. Other ideals are non-prime.

Proof.

If $n = ab$ with $1 < a, b < n$ then $ab \in (n)$ but $a, b \notin (n)$, so (n) is not prime.
If p is prime then $n \in (p)$ iff $p|n$; hence $ab \in (p)$ iff $p|ab$ iff $p|a$ or $p|b$. □

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Theorem

I is prime iff R/I is a domain.

Proof.

$xy \in I$ iff $(x+I)(y+I) = (0+I)$. □

Lemma

Let $n \geq 2$. $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$ is a domain iff n is prime.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Definition

I is maximal if it is a proper ideal not properly contained in any other proper ideal.

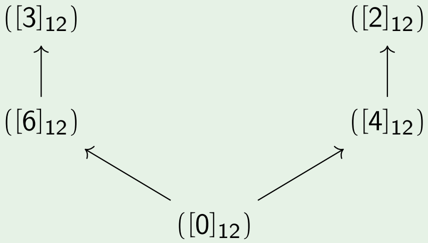
Example

Consider again (we gave this example to illustrate the correspondence theorem) the proper ideals of $\mathbb{Z}_{12}$. These are all principal, namely

$$([3]_{12}) = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\},$$
$$([2]_{12}) = \{[0]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\},$$
$$([6]_{12}) = \{[0]_{12}, [6]_{12}\}, \qquad ([4]_{12}) = \{[0]_{12}, [4]_{12}, [8]_{12}\}, \qquad ([0]_{12}) = \{[0]_{12}\}$$

and are contained in each other as follows:

Example (contd.)



The maximal ideals are $([3]_{12})$ and $([2]_{12})$.

Theorem

If I contains a unit, then $I = R$.

Proof.

Let $r \in I$ be a unit. Then $1 = r^{-1}r \in I$. Hence, for any $s \in R$, $s = 1s \in I$. □

Theorem

R is a field iff its only ideals are $(0), (1)$.

Proof.

Suppose R field, and $I \neq (0)$ an ideal. Then I contains a unit, so $I = (1)$. Conversely, suppose that $(0), (1)$ are the only ideals in R. Take $r \neq 0$. The ideal $I = (r)$ is non-zero, so $I = (1)$. Since $1 \in I$, $1 = sr$ for some $s \in R$. Hence r is a unit. □

Corollary

R is a field iff (0) is maximal.

Theorem

I is maximal iff R/I is a field.

Proof.

R/I is a field iff its only proper ideal is the zero ideal. By the correspondence theorem, this happens iff the only proper ideal containing I is I. □

Theorem

The maximal ideals in $\mathbb{Z}$ are (p) for p prime.

Theorem

Any maximal ideal is prime. If R is finite, then any prime ideal is maximal.

Proof.

Fields are domains; finite domains are fields. □

Definition

R is local if it has a unique maximal ideal.

Example

$\mathbb{Z}$ is not local; $\mathbb{Z}_4$ is.

Example

Any field is local.

Theorem

If the set of non-units in R form an ideal I, then I is maximal, and R is local.

Proof.

If $I \subsetneq J$, take $r \in J \setminus I$. Then r is a unit, so $J = R$. Hence I is maximal. If L is any proper ideal in R it consists exclusively of non-units, hence is contained in I. □

Example

Let $R = \mathbb{Q}[[x]]$, the set of formal power series in one indeterminate, with coefficients in $\mathbb{Q}$. A general element is

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots, \qquad a_j \in \mathbb{Q}$$

We have that

$$(1 + x + x^2 + x^3 + \dots)(1 - x) = 1,$$

so $(1-x)^{-1} = 1+x+x^2+x^3+\dots$, and $(1+x+x^2+x^3+\dots)^{-1} = 1-x$. In general, we claim that $f(x)$ is invertible iff $a_0 \neq 0$.

Example (cont)

To see this, consider

$$(a_0 + a_1 x + a_2 x^2 + \dots)(b_0 + b_1 x + b_2 x^2 + \dots) = 1$$

This is solvable for the b_i's iff $a_0 \neq 0$; collecting powers of x we have

$$\begin{aligned} a_0 b_0 &= 1 \\ a_1 b_0 + a_0 b_1 &= 0 \\ a_2 b_0 + a_1 b_1 + a_0 b_2 &= 0 \\ &\vdots \end{aligned}$$

which can be solved inductively iff $a_0 \neq 0$.
Let I denote the set of power series with zero constant term. Then $I = (x)$, a principal ideal. So I is maximal, and R is local.

Example

Let $R = \mathbb{Q}[x]$, and let $I = (x^2 + 1)$. Then I is prime. Put $T = \left\{ \frac{f(x)}{g(x)} \middle| f(x) \in R,\, g(x) \in R \setminus I \right\}$. Check that this is a ring! We claim that T is local, with the unique maximal ideal

$$J = \left\{ \frac{f(x)}{g(x)} \middle| f(x) \in I,\, g(x) \in R \setminus I \right\}$$

1. If $f(x), g(x) \notin I$ then $\frac{1}{\frac{f(x)}{g(x)}} = \frac{g(x)}{f(x)}$, so anything outside J is invertible.
2. If $\frac{f(x)}{g(x)}$, with $g(x) \notin J$, is invertible then exists $\frac{h(x)}{k(x)}$ with $k(x) \notin J$ such that

$$\frac{f(x)h(x)}{g(x)k(x)} = 1 \quad \implies f(x)h(x) = g(x)k(x).$$

   Since $g(x)k(x) \notin I$ we have that $f(x) \notin I$. So anything invertible is outside J.

   Since J consists precisely of the non-units, and is an ideal, it is the unique maximal ideal.

Definition

If I, J are ideals in R, then their sum

$$I + J = \{\, i + j | i \in I, j \in J \,\}$$

is the smallest ideal containing both. When $I = (i)$, $J = (j)$ are both principal, we write

$$(i) + (j) = (i, j),$$

and similarly for *finitely generated* ideals.

Example

In $\mathbb{C}[x, y]$ we have that $(x^3, xy) + (x^2y, y^4) = (x^3, xy, y^4)$ (picture)

Definition

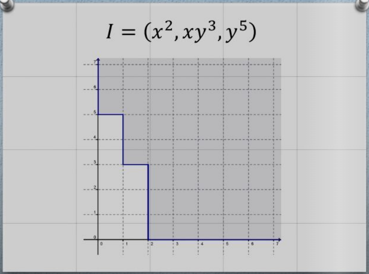
If $R = K[x_1, \ldots, x_n]$, where K is a field, then a monomial is an element of the form $x_1^{a_1} \cdots x_n^{a_n}$, and a monomial ideal is an ideal I which satisfies the following equivalent conditions:

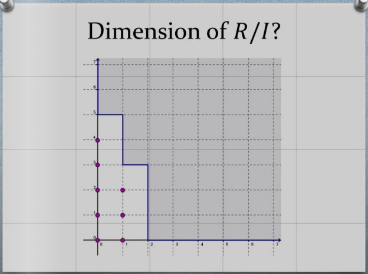
- $I = (m_1, \ldots, m_r)$ where the m_i's are monomials
- If $f = \sum_m c_m m \in R$ then $f \in I$ iff all monomials $m \in I$.
- As a K-vector space, I has a basis consisting of monomials.

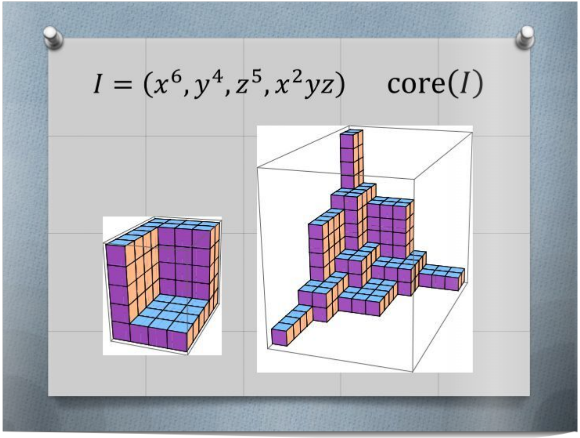
So a monomial ideal is determined by the monomials contain therein; in fact, those monomials form a monoid ideal of the monoid of monomials (under multiplication).

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET






$I = (x^6, y^4, z^5, x^2yz)$
core(I)

Definition

If I, J are ideals in R, then their intersection $I \cap J$ is the largest ideal contained in both.

Example

In $\mathbb{C}[x, y]$ we have that

$$(x^3, xy) \cap (x^2y, y^4) = (xy^4, x^2y)$$

(picture)

Definition

If I, J are ideals in R, then, by abuse of notation, IJ denotes the ideal generated by the set IJ, i.e., all finite sums of elements in IJ:

$$\left\{ \sum_{k=1}^{r} i_k j_k \middle| 1 \leq r < \infty,\ i_k \in I,\ j_k \in J \right\}$$

Lemma

$IJ \subseteq I \cap J$.

Example

In $\mathbb{C}[x, y]$ we have that

$$(x^3, xy)(x^2y, y^4) = (x^5y, xy^5, x^3y^2)$$

Definition

If I is an ideal in R, then its *radical* is

$$\sqrt{I} = \{\, r \in R \,|\, r^n \in I \text{ for some } n > 0 \,\}$$

The ideal I is radical if it equals its radical.

Theorem

- $I \subseteq \sqrt{I} = \sqrt{\sqrt{I}}$
- *I is radical if and only if R/I is reduced, i.e., lacks nilpotent elements*

Example

In $\mathbb{C}[x, y]$ we have that

$$\sqrt{(x^3, xy)} = (x)$$

Definition

I is a *primary* ideal if

$$xy \in I \implies x \in I \text{ or } y \in \sqrt{I}$$

Lemma

I is primary iff all zero-divisors of R/I are nilpotent.

Example

In $\mathbb{C}[x, y]$ we have that (x^3, xy) is not primary, since $x * y \in I$, $x \notin I$, $y \notin \sqrt{I}$. However, the ideal can be decomposed as an intersection of primary ones:

$$(x^3, xy) = (x) \cap (x^3, y)$$

Recall that all ideals in $\mathbb{Z}$ are principal.

Theorem

For non-zero ideals of $\mathbb{Z}$ it holds that

1. $(n) \subseteq (m)$ *iff* $m|n$
2. $(n) + (m) = (\gcd(n, m))$
3. $(n) \cap (m) = (\mathrm{lcm}(n, m))$
4. $(n)(m) = (nm)$
5. $\sqrt{(p_1^{a_1} \cdots p_r^{a_r})} = (p_1 \cdots p_r)$
6. (n) *is prime iff* (n) *is maximal iff* n *is a prime number.*
7. (n) *is radical iff* n *is square-free*
8. (n) *is primary iff* n *is a prime power*

Proof.

1. If $n = ms$ then $n \in (m)$ hence $(n) \subseteq (m)$. Conversely if $(n) \subseteq (m)$ then $n \in (m)$ hence $n = ms$.
2. Put $d = \gcd(n, m)$. Then $d|n$, $d|m$, so $(n) \subseteq (d)$, $(m) \subseteq (d)$. But $(n) + (m)$ is the smallest ideal containing (n) and (m), so $(n) + (m) \subseteq (d)$.
   Conversely, by Bezout, $d = xn + ym \in (n) + (m)$, so $(d) \subseteq (n) + (m)$.
3. Put $\ell = \operatorname{lcm}(n, m)$. Then $\ell = an$, $\ell = bm$, so $\ell \in (n) \cap (m)$, hence $(\ell) \subseteq (n) \cap (m)$.
   Conversely, if $s \in (n) \cap (m)$ then $s = xn$, $s = ym$ so it is a common multiple of n and m, hence divisible by ℓ. It follows that $s \in (\ell)$.

□