Abstract Algebra, Lecture 10

Introduction to 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

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

1. **Rings, definitions and types**
   - Division rings and domains
2. **New rings from old**
   - Direct products
   - Group rings
   - Semigroup rings
   - Algebras
3. **Subrings, ideals, homomorphisms, quotients**
4. **The isomorphism theorems**
5. **The correspondence theorem**

Summary

Definition

A ring $(R, +, 0, *)$ is an abelian group $(R, +, 0)$, written additively, and an associative multiplication $*$ on the underlying set R, satisfying the *distributive laws*

$$a * (b + c) = a * b + a * c$$
$$(b + c) * a = b * a + c * a$$

for all $a, b, c \in R$.
The ring is *unitary* if there is a (necessarily unique) multiplicative unit $1 = 1_R \neq 0 =_R$ such that $1 * a = a * 1 = a$ for all $a \in R$.
It is *commutative* if $a * b = b * a$ for all $a, b \in R$. (Note that $a + b = b + a$ always holds in any ring).

Example

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative, unitary rings, with standard addition and multiplication.
$2\mathbb{Z}$ is a commutative, but not unitary, ring.

Example

The set $M_n(\mathbb{R})$ of $n \times n$ real matrices is a unitary, but not commutative, ring under standard matrix addition and multiplication.
The subset $\mathrm{GL}_n(\mathbb{R})$ of invertible matrices is not a ring (not closed under addition).

Definition

An element $R \ni r \neq 0$ is a

- *zero-divisor*, if $rs = 0$ or $sr = 0$ for some $R \ni s \neq 0$,
- *unit* if there is a (necessarily unique) $R \ni s \neq 0$ such that $sr = rs = 1$. (Obviously, this concept is only relevant for unitary rings)
- *nilpotent*, if $r^n = r * r * \cdots * r = 0$ for some positive integer n,
- *idempotent*, if $r^2 = r$

Nilpotent element are zero-divisors, since $r^{n-1} * r = 0$, and so are (most) idempotents in a unitary ring, since $r(r-1) = 0$.

Example

Let $R = M_2(\mathbb{Q})$.

- $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is a unit, with inverse $\begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$
- $B = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ is a zero-divisor, as is $C = \begin{pmatrix} 2 & 2 \\ -1 & -1 \end{pmatrix}$, since
  $B * C = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $C * B = \begin{pmatrix} 4 & 8 \\ -2 & -4 \end{pmatrix}$.
- $D = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent, since $D * D = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
- $E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is idempotent, since $E * E = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Definition

The set of all units in an unitary ring R is denoted by R^*, or sometimes $\mathcal{U}(R)$. It is a group under multiplication, and is called the multiplicative group of R.

Example

- $M_n(\mathbb{Q})^* = \mathrm{GL}_n(\mathbb{Q})$
- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
- $\mathbb{Z}^* = \{-1, 1\}$
- $\mathbb{Z}_n^* = \{\, [k]_n | \gcd(k, n) = 1 \,\}$.

Lemma

Let R be a commutative unitary ring.

- *The set of idempotent elements is closed under multiplication.*
- *The set of nilpotent elements is closed under multiplication, closed under addition, and is absorbing: the product of a nilpotent element and a general ring element is nilpotent.*
- *The set of zero-divisors is closed under multiplication.*

Definition

A unitary ring R is a *division ring* if $R^* \cup \{0\} = R$.
A commutative division ring is a *field*, whereas a non-commutative division ring is a *skew field*.

Example

$\mathbb{Q}$ is a field.
The *quaternions* $\mathbb{H}$ is a skew field. The quaternions can be given as

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \middle| z, w \in \mathbb{C} \right\}$$

They can also be given as the 4-dimensional $\mathbb{R}$-vector space with basis $1, i, j, k$, with multiplication determined by the relations

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j$$

Definition

A commutative, unitary ring R is an integral domain if it has no non-zero zerodivisors.

Example

- $\mathbb{Z}$ is a domain.
- $\mathbb{Z}_5$ is a domain.
- $\mathbb{Z}_6$ is not a domain, since $[2]_6 * [3]_6 = [6]_6 = [0]_6$.
- Any field is a domain.

Lemma

Let $n > 1$ be an integer. $\mathbb{Z}_n$ is a domain iff it is a field iff n is prime.

Proof.

The equation

$$ax \equiv 1 \mod n$$

has a solution mod n iff $\gcd(a, n) = 1$. Thus, if n is prime, there is a solution, and $[a]_n \neq [0]_n$ has an inverse. Hence $\mathbb{Z}_n$ is a field, and thus a domain.

If $n = rs$ is composite, then $[r]_n[s]_n = [rs]_n = [n]_n = [0]_n$, so there are zero-divisors. □

Theorem

A finite integral domain R is a field.

Proof.

- Put $R' = R \setminus \{0\}$
- Take $r \in R'$
- Multiplication map $R' \ni x \mapsto rx$
- Image in R' since R domain, thus r non-zero-divisor
- Map injective, since if $rx = ry$ then $r(x - y) = 0$, so $x - y = 0$
- Set-theoretic fact: injective map from finite set to itself is a bijection!
- Thus, in particular, 1_R is in the image of the map
- Thus exist $x \in R'$ with $rx = 1$
- So r is a unit

□

Definition

If R, S are rings, then their *direct product* is

$$R \times S = \{ (r,s) | r \in R, s \in S \}$$

with component-wise operations.

Example

$\mathbb{Z} \times \mathbb{Z}$ is a unitary, commutative ring. It is not a domain, since

$$(1,0) * (0,1) = (0,0)$$

Definition

Let R be a commutative, unitary ring, and let G be a group. The group ring over G with coefficients in R is

$$R[G] = \left\{ c \in R^G \,\middle|\, c(g) = 0_R \text{ for all but finitely many } g \in G \right\}$$

with component-wise addition, *scaling* $(\lambda c)(g) = \lambda c(g)$, and convolution product

$$(c * d)(g) = \sum_{\{ (x,y) \in G \times G \mid x *_G y = g \}} c(x) *_R d(y)$$

Example

Let $G = S_3$, $R = \mathbb{Q}$. Then an arbitrary element in $\mathbb{Q}[S_3]$ can be written as

$$f = c_{()}() + c_{(12)}(12) + c_{(13)}(13) + c_{(23)}(23) + c_{(123)}(123) + c_{(132)}(132)$$

We have, for instance that

$$\big((1,2) + 2(1,3,2)\big) * \big(3(1,2,3) + 5(1,3)\big) = 6 + 10(2,3) + 5(1,2,3) + 3(1,3)$$
$$\big(3(1,2,3) + 5(1,3)\big) * \big((1,2) + 2(1,3,2)\big) = 6 + 3(2,3) + 10(1,2) + 5(1,3,2)$$

While these two elements do not commute, there are idempotents that commute with everything; for instance,

$$2 - (1,2,3) - (1,3,2)$$

Definition

We can replace the group G by a semigroup M in the definition of a group ring, and obtain instead a *semigroup ring* $R[G]$

Example

Let $R = \mathbb{Z}$, $M = 2\mathbb{N}$. Then $\mathbb{Z}[M]$ is the set of polynomials $f(t^2)$ with integer coefficients and only even powers of t occuring.
Let N denote the semigroup of natural numbers ≥ 3, under multiplication. The convolution multiplication in $\mathbb{Z}[N]$ is illustraded below:

$$(2*t^3 - 11t^4)*(5*t^3 + 3*t^4) = 2*5*t^9 + 2*3*t^{12} - 11*5*t^{12} - 11*3*t16 =$$
$$= 10t^9 - 49t^{12} - 33t^{16}$$

Jan Snellman
TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Definition

Let K be a field, and V be a vector space over K. Suppose that

1. $K \subset V$
2. There is an associative multiplication $*$ on V which makes V a ring

then V is called a K-algebra.

Equivalently, a commutative, unitary ring is a K-algebra if there is an injective ring homomorphism $K \hookrightarrow V$.

Example

- The group algebra $\mathbb{Q}[S_3]$ is a $\mathbb{Q}$-algebra (embedd $r \in \mathbb{Q}$ as $r()$)
- The semigroup ring $\mathbb{Q}[\mathbb{N}] = \mathbb{Q}[t]$, the polynomial ring in one indeterminate, with coefficients in $\mathbb{Q}$, is a $\mathbb{Q}$-algebra. Embedd the rationals as constant polynomials.
- More generally, the polynomial ring in several variables $\mathbb{Q}[t_1, \ldots, t_r]$ is a $\mathbb{Q}$-algebra.
- One can also construct the non-commutative polynomial ring

$$\mathbb{Q}\langle t_1, \ldots, t_r \rangle = \mathrm{Span}_{\mathbb{Q}}\{ \text{ words in } t_1, \ldots, t_r \}$$

- There are also power series rings $\mathbb{Q}[[t]]$, $\mathbb{Q}[[t_1, \ldots, t_r]]$, which are all $\mathbb{Q}$-algebras.

Example

If the K-vector space V has an ordered basis $e_1, \ldots, e_n$, then an algebra multiplication $*$ on V is determined (by the distributive laws) by the values of

$$e_i * e_j = \sum_{k=1}^{n} c_{i,j,k} e_k$$

The n^3 *structure constants* $c_{i,j,k}$ can not be chosen arbitrarily; associativity imposes conditions.
For instance, if $n = 2$, then

$$\begin{aligned}
e_1 * e_1 &= a e_1 + b e_2 \\
e_1 * e_2 &= c e_1 + d e_2 \\
e_2 * e_1 &= e e_1 + f e_2 \\
e_2 * e_2 &= g e_1 + h e_2
\end{aligned}$$

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Example (cont.)

but

$$e_1 * (e_2 * e_1) = (e_1 * e_2) * e_1$$

so

$$\begin{aligned} LHS &= e_1 * (ee_1 + fe_2) = ee_1 * e_1 + fe_1 * e_2 = e(ae_1 + be_2) + f(ce_1 + de_1) \\ &= (ae + cd)e_1 + (be + df)e_2 = RHS = (e_1 * e_2) * e_1 \\ &= (ce_1 + de_2) * e_1 = ce_1 * e_1 + de_2 * e_1 \\ &= c(ae_1 + be_1) + d(ee_1 + fe_2) = (ac + de)e_1 + (bc + df)e_2 \end{aligned}$$

so we get two conditions (there are more) for the structure constants:

$$\begin{aligned} ae + cf &= ac + de \\ be + df &= bc + df \end{aligned}$$

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Example

The quaternions can be given by structure constants:

$$
\begin{aligned}
1 * 1 = 1 &= 1 * 1 + 0 * i + 0 * j + 0 * k \\
1 * i = i * 1 = i &= 0 * 1 + 1 * i + 0 * j + 0 * k \\
1 * j = j * 1 &= j \\
1 * k = k * 1 &= k \\
i * i &= -1 \\
i * j &= k \\
i * k &= -j
\end{aligned}
$$

et cetera.

Definition

Let R be a ring. Then $S \subseteq R$ is a subring of R if it is a ring with the restricted operations from R; equivalently, if it is a subgroup of the additive group, and if

$$SS \subseteq S$$

We write $S \leq R$.

Lemma

Any subring of a field is a domain.

Proof.

The overring has no zerodivisors. □

Example

$$2\mathbb{Z} \le \mathbb{Z} \le \mathbb{Q} \le \mathbb{R} \le \mathbb{C} \le \mathbb{H}$$

In particular, we see that subrings of fields need not be fields.

Example

Let $R = \mathrm{M}_3(\mathbb{Q})$ and

$$S = \left\{ \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{bmatrix} \middle| a, b, c, d \in \mathbb{Q} \right\}$$

Then $S \le R$. Not that S is unitary, but $1_S \neq 1_R \notin S$.

Center

Definition

The *center* $Z(R)$ of a ring R consists of all elements x such that $xy = yx$ for all $y \in R$.

Lemma

$Z(R) \leq R$.

Proof.

Suppose that $a, b \in \mathbb{Z}(R$ and that $r \in R$. Then

$$(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab)$$

and

$$(a+b)r = ar + br = ra + rb = r(a+b).$$

□

Example

- If R is commutative, then $Z(R) = R$.
- $Z(M_3(\mathbb{Q})) = \left\{ \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix} \middle| c \in \mathbb{Q} \right\}$
- The center of a skew-field is a field
- If $Z(R)$ is a field the R is a $Z(R)$-algebra.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Example

For finite dimensional algebras, the center can be found via linear algebra. There are also numerous interesting results for more structured algebras, such as group rings over a field. See if you can guess what the center of such an algebra is from the following example!

```
sage: R = GroupAlgebra(SymmetricGroup(4),QQ)
sage: R.center_basis()
((), (3,4) + (2,3) + (2,4) + (1,2) + (1,3) + (1,4),
    (1,2)(3,4) + (1,3)(2,4) + (1,4)(2,3), (2,3,4) +
    (2,4,3) + (1,2,3) + (1,2,4) + (1,3,2) + (1,3,4) +
    (1,4,2) + (1,4,3), (1,2,3,4) + (1,2,4,3) +
    (1,3,4,2) + (1,3,2,4) + (1,4,3,2) + (1,4,2,3))
```

Definition

Let R be a ring. Then $S \subseteq R$ is a (twosided) ideal of R if it is a subring and

$$SR \subseteq S$$
$$RS \subseteq S$$

The ideal $\{0\}$ is called trivial, the ring itself is an improper ideal.

Example

The proper, non-trivial ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ with $n > 1$ an integer.

Example

A field has no proper, non-trivial ideals.

Definition

Let R be a ring. Then $S \subseteq R$ is a left ideal of R if is a subring and if

$$RS \subseteq S$$

S is a right ideal of R if it is a subring and if

$$SR \subseteq S$$

Example

The left annihilator of an element $f \in R$ is the set $\{g \in R | g * f = 0\}$. It is a left ideal.

```
sage: R = GroupAlgebra(DihedralGroup(4),QQ)
sage: rb = R.basis().list()
sage: f = rb[0] - rb[1]
sage: f
() - (1,3)(2,4)
sage: rab = R.annihilator_basis([f])
sage: rab[0]
() + (1,3)(2,4)
sage: rab[0]*f
0
```

Definition

Let R, S be rings. A map

$$\phi : R \to S$$

is a *ring homomorphism* if, for all $a, b \in R$,

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$

Example

$$\phi : \mathbb{Z} \to \mathbb{Z}_n$$
$$\phi(k) = [k]_n$$

is a (surjective) ring homomorphism.

Example

$$\xi : \mathbb{Z} \to \mathbb{Z}$$
$$\xi(k) = 2k$$

is *not* a ring homomorphism.

Example (Svensson)

$$F : \mathbb{Z}_2 \to \mathbb{Z}_6$$
$$F([0]_2) = [0]_6$$
$$F([1]_2) = [3]_6$$

is a ring homomorphism.

Theorem

Let $\phi : R \to S$ be a ring homomorphism.

1. $\phi(O_R) = 0_S$, $\phi(-r) = -\phi(r)$,
2. $\phi(r^k) = \phi(r)^k$ *for all positive integers* k
3. $\phi(R')$ *is a subring of* S *whenever* $R' \leq R$
4. $\phi^{-1}(S')$ *is a subring of* R *whenever* $S' \leq S$
5. *If* R *is unitary, and if* $\phi(R)$ *is non-trivial, then* $\phi(1_R)$ *is the multiplicative identity in the subring* $\phi(R) \leq S$
6. *If* R *is unitary, and if* $\phi(R)$ *is non-trivial, then* $\phi(r)$ *is a unit in* $\phi(R)$ *whenever* r *is a unit in* R*. In this case,* $\phi(r)^{-1} = \phi(r^{-1})$.

As the previous example shows, 1 need not be sent to 1, unless ϕ is surjective.

Example

Study once again $R = \mathrm{M}_3(\mathbb{Q})$ and

$$S = \left\{ \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{bmatrix} \middle| a, b, c, d \in \mathbb{Q} \right\}$$

Let ϕ be the inclusion map; it is a ring homomorphism, and

$$\phi(1_S) = \phi\left(\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \neq 1_R.$$

Theorem

Let $\phi : R \to S$ be a ring homomorphism. Then the kernel

$$\ker \phi = \phi^{-1}(\{0\})$$

is an ideal in R.

Proof.

The inverse image of a subring is a subring, so suffices to show that if $k \in \ker \phi$, $r \in R$ then $kr \in \ker \phi$ and $rk \in \ker \phi$. But $\phi(rk) = \phi(r)\phi(k) = \phi(r) * 0 = 0$ since $k \in \ker \phi$, and so $rk \in \ker \phi$. The case for kr is similar. □

Theorem

If $I \subseteq R$ is an ideal, then the set of left cosets $r + I$, $r \in R$, becomes a ring with the (well-defined) operations

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

This quotient ring is denoted R/I.

Proof.

We know that it is an abelian group; let's check that multiplication is well-defined (distributivity is inherited).
If $r_1 - r_2 \in I$, $s_1 - s_2 \in I$ then

$$r_2 * s_2 = (r_1 + i_1) * (s_1 + i_2) = r_1 * s_1 + r_1 * i_2 + i_1 * s_1 + i_1 * i_2 = r_1 * s_1 + j$$

with $j \in I$. □

Theorem

Let $\phi : R \to S$ be a ring homomorphism. The relation on R defined by

$$r_1 \sim r_2 \quad \iff \quad \phi(r_1) = \phi(r_2)$$

satisfies

1. $\sim$ *is an equivalence relation*
2. $\sim$ *respects addition and multiplication*
3. *Addition and multiplication of equivalence classes via the corresponding operations on representatives is well defined and turns the set of equivalence classes into a ring*
4. $[0]_\sim = \ker \phi$
5. $[r]_\sim = r + \ker \phi$, *i.e., the equivalence classes are cosets of the kernel*

Theorem

Let $I \subseteq R$ be an ideal. Define the canonical quotient epimorphism by

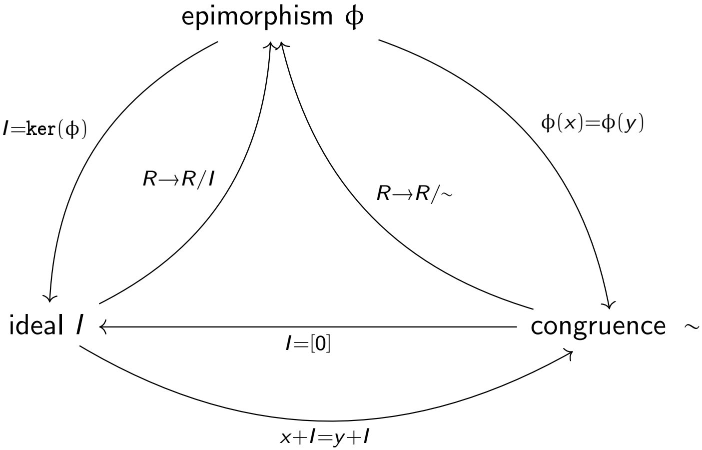
$$\pi : R \to R/I$$
$$\pi(r) = r + I$$

Then

1. $\ker \pi = I$,
2. *The quotient ring obtained from the kernel congruence is equal to R/I*

In other words, similar to the situatin for groups, with "normal subgroups" replaced by "ideals", we have that quotient ring, epimorphism, ideals, and congruences, are very tightly related.

Epimorphisms, ideals, congruences



Theorem

Let $\phi : R \to S$ be a ring homomorphism. Then $\phi(R)$ is a subring of S, and

$$\phi(S) \simeq \frac{R}{\ker \phi}$$

In particular, if ϕ is surjective, then $S \simeq R/I$.

Proof.

Similar to the group case. □

Just as for groups, in order to understand a quotient ring R/I, we guess a candidate for what we thing it should be, and then try to find a surjective ring homomorphism to the candidate that kills off precisely the elements of I.

Example

Let $R = \mathbb{R}^{\mathbb{R}}$, the set of all real-valued functions on $\mathbb{R}$. This becomes a unitary, commutative ring under component-wise addition and multiplication:

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

The function which is constant one, $\chi_{\mathbb{R}}$, is the multiplicative identity, and the constantly zero function $\chi_{\emptyset}$ is the additive identity.
Any function $f(x)$ with a zero, $f(a) = 0$, is a zero divisor, since $f * \chi_{\{a\}}$ is constant zero. Functions without a zero are units.
The set $I(a)$ of functions vanishing at a is an ideal (easy check). So what is $R/I(a)$?

Example (contd.)

The elements of $R/I(a)$ are cosets $f + I(a)$, where f is a function; two such functions are equivalent modulo $I(a)$ if their difference lies in $I(a)$, that is, if they have the same value at a. A coset $f + I(a)$ should thus be charactersized with the value $f(a)$, a single real number.
We hence guess that $R/I(a) \simeq \mathbb{R}$. Now to prove this.
How can we define a surjective ring homomorphism $\phi : R \to \mathbb{R}$ killing of precisely those functions that vanish at a? We try

$$\phi : R \to \mathbb{R}$$
$$\phi(f) = f(a)$$

that is, *evaluating* f at a. We check that this is a ring homomorphism.
Clearly, ϕ is surjective, and kills precisely $I(a)$.
By the first isomorphism thm,

$$R/I(a) \simeq \mathbb{R}$$

Example

Let $I \subset M_n(\mathbb{Z})$ consists of all matrices whose every entry is even. Is I an ideal, and if so, what is the quotient?

The map

$$M_n(\mathbb{Z}) \ni (a_{i,j}) \mapsto ([a_{i,j}]_2) \in M_n(\mathbb{Z}_2)$$

is a surjective ring homomorphism (check!) with kernel I. Hence,

$$\frac{M_n(\mathbb{Z})}{I} \simeq M_n(\mathbb{Z}_2).$$

Example

Consider the matrix

$$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Consider the smallest subring $R \subseteq \mathrm{Mat}_2(\mathbb{Q})$, of the ring all 2-by-2 matrices with rational entries, that contains M. This subring, by definition, contains $I, M, M^2, \ldots$, and all linear combinations of these. Does it also contain M^{-1}?

Example (Cont.)

Let us introduce the ring homomorphism

$$\phi : \mathbb{Q}[x] \to \mathrm{Mat}_2(\mathbb{Q})$$
$$\phi(g(x)) = g(M)$$

Then, by definition, $R = \phi(\mathbb{Q}[x])$, and by the first iso thm

$$R \simeq \frac{\mathbb{Q}[x]}{I}$$

where $I = \ker \phi$.
We'll talk about the ring $\mathbb{Q}[x]$ in great detail in later lectures, and among other thing prove that all ideals are *principal*; i.e.,

$$I = (f(x)) = \{\, f(x)h(x) \,|\, h(x) \in \mathbb{Q}[x] \,\}$$

Example (Cont.)

In this particular case, $I = (x^2 - 5x - 2)$, where the generator is the *minimal polynomial* for M (it happens to coincide with the characteristic polynomial in this case; it is always a factor).
What does this mean? Since $x^2 - 5x - 2$ is irreducible, $R \simeq \frac{\mathbb{Q}[x]}{I}$ is a field (we will prove this) so in particular, $M^{-1} \in R$ since $M \in R$. And in fact, since

$$\phi(x^2 - 5x - 2) = M^2 - 5M + 2I = 0,$$

it holds that

$$2I = 5M - M^2 = M(5I - M),$$

so

$$M^{-1} = \frac{5}{2}I - \frac{1}{2}M \in R$$

Definition

Let R be a unitary commutative ring. The characteristic $\mathtt{char}(R)$ is the smallest positive integer n such that $n1 = 1 + \cdots + 1 = 0$ (n times). If no such n exists, we say that $\mathtt{char}(R) = 0$.

Lemma

If $\mathtt{char}(R) = n > 0$ *then*

$$nr = \underbrace{r + \cdots + r}_{n \text{ times}} = 0$$

Proof.

Distributivity. □

Lemma

Let R be a commutative unitary ring. The subring S generated by 1 is isomorphic to $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$ if R has characteristic $n > 0$, and to $\mathbb{Z}$ if R has characteristic 0

Proof.

Consider

$$\phi : \mathbb{Z} \to R$$

$$\phi(k) = k1_R$$

Then $n = \mathrm{char}(R)$ is the smallest positive integer in $\ker \phi$ if $\mathrm{char}(R) = n > 0$, and hence $\ker \phi = n\mathbb{Z}$, so by the first iso thm $S \simeq \mathbb{Z}/n\mathbb{Z}$.

If $\mathrm{char}(R) = 0$ then $\ker \phi = \{0\}$, so ϕ is injective and $S \simeq \mathbb{Z}$. □

Theorem (Second iso thm)

Let R be a ring, S be a subring of R, and let I be an ideal of R. Then $S+I$ is a subring of R, and I is an ideal of that subring, and

$$\frac{S+I}{I} \simeq \frac{S}{S \cap I}$$

Example

$$\frac{2\mathbb{Z}}{6\mathbb{Z}} = \frac{4\mathbb{Z}+6\mathbb{Z}}{6\mathbb{Z}} \simeq \frac{4\mathbb{Z}}{4\mathbb{Z} \cap 6\mathbb{Z}} = \frac{4\mathbb{Z}}{12\mathbb{Z}}$$

Theorem (Third iso thm)

Let R be a ring, and let I, J be ideals of R. If $J \subseteq I$ then I/J is an ideal in the quotient ring R/J, and

$$\frac{R/J}{I/J} \simeq \frac{R}{I}$$

Example

$$\frac{\mathbb{Z}/(12\mathbb{Z})}{(4\mathbb{Z})/(12\mathbb{Z})} \simeq \frac{\mathbb{Z}}{(4\mathbb{Z})}$$

Example

Let $R = \mathbb{Q}[x]$, $g(x) = x^3 - 1$, $f(x) = x^2 + x + 1$, $J = (g(x))$, $I = (f(x))$. Then $J \leq I$ since $f(x)|g(x)$, and

$$\frac{R/J}{I/J} \simeq \frac{R}{I} = \frac{\mathbb{Q}[x]}{(x^2 + x + 1)}$$

which is a $\mathbb{Q}$-algebra with basis $1, \bar{x}$ and structure constants

$$1 * \bar{x} = \bar{x}, \quad \bar{x} * \bar{x} = -1 - \bar{x}.$$

On the other hand, $\frac{R}{J} = \frac{\mathbb{Q}[x]}{(x^3-1)}$ is a $\mathbb{Q}$-algebra with basis $1, \bar{x}, \bar{x}^2$. In this quotient ring, I/J is a principal ideal generated by $\bar{x}^2 + \bar{x} + 1$.

Theorem (Correspondence thm)

Let R be a ring, and let I be an ideal of R. Let $\pi : R \to R/I$ be the canonical quotient epimorphism. The maps

$$J \mapsto \pi(J) = J/I$$

and

$$L \mapsto \pi^{-1}(L)$$

establish an inclusion-preserving bijection between ideals in R containing I, and ideals of R/I.

Proof.

Just like for groups. □

Example

The ideals of $\mathbb{Z}$ are all of the form $(n) = n\mathbb{Z}$, with $0\mathbb{Z} \subseteq n\mathbb{Z} \subseteq 1\mathbb{Z}$ for all n, and for positive n, m,

$$(n) \subseteq (m) \iff m|n$$

What are the ideals of $\mathbb{Z}_{12} = \frac{\mathbb{Z}}{12\mathbb{Z}}$?
Well, the divisors of 12 are $1, 2, 3, 4, 6, 12$, so the ideals containing $12\mathbb{Z}$ are

$$\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z},$$

and the (proper) ideals in $\frac{\mathbb{Z}}{12\mathbb{Z}}$ are thus

$$\frac{2\mathbb{Z}}{12\mathbb{Z}}, \frac{3\mathbb{Z}}{12\mathbb{Z}}, \frac{4\mathbb{Z}}{12\mathbb{Z}}, \frac{6\mathbb{Z}}{12\mathbb{Z}}, \frac{12\mathbb{Z}}{12\mathbb{Z}}.$$

Example

Let $R = \mathbb{Q}[x]$, and let $I = (x^3)$ be the principal ideal generated by x^3. We shall prove later on that all (proper) ideals $J \supset I$ are of the form $J = (g(x))$, where $g(x)$ is a divisor of x^3; hence these ideals are

$$(x^3) \subset (x^2) \subset (x).$$

Thus the ideals of R/I are

$$(0) = (x^3)/I \subset (x^2)/I \subset (x)/I.$$