IDEALS

MATEUSZ MICHAŁEK

Definition 0.1 (Ring, Ideal, Unit, Nilpotent, Zero-divisor, Integral ring, Field)**.** *A* ring *will be a commutative ring with $1 \neq 0$.*

An ideal *I of a ring R is a nonempty subset for which:*

$$I + I := \{i + j : i, j \in I\} \subset I \quad RI := \{ri : r \in R, i \in I\} \subset I.$$

An ideal I is proper *if $I \neq R$. To indicate that a subset I is an ideal we will write $I \lhd R$.*

A unit *is an element of a ring that has a multiplicative inverse. The set of all units $U(R)$ of a ring R is an abelian group.*

A ring is a field *if and only if $U(R) = R \setminus \{0\}$.*

A nilpotent *is an element $r \in R$ for which $r^n = 0$ for some integer n. The set of all nilpotents will be denoted by* $\mathrm{nil}(R)$.

A zero-divisor *is an element $r \in R$ for which there exist such a nonzero $s \in R$ that $sr = 0$. The set of all zero-divisors will be denoted by $D(R)$.*

A ring is integral *if and only if $D(R) = \{0\}$.*

The proof of the following lemma is the first exercise.

Lemma 0.2. *(i) $U(R) + \mathrm{nil}(R) = U(R)$*

(ii) The following conditions are equivalent:
- *R is a field;*
- *R has only two ideals: (0) and R;*
- *every morphism from R is injective.*

The following are basic operations on ideals.

- Let $I_1, \dots, I_k$ be a finite collection of ideals and let $(I_\lambda)_{\lambda \in \Lambda}$ be an arbitrary (possibly infinite) collection indexed by elements of a set Λ. We define:
  - sum of finitely many ideals: $I_1 + \dots + I_k := \{i_1 + \dots + i_k : i_j \in I_j\}$;
  - intersection of ideals: $\bigcap_{\lambda \in \Lambda} I_\lambda$;
  - ideal generated by a set $S \subset R$: $(S) := \bigcap_{S \subset I} I$, where the intersection is taken over all ideals I that contain S;
  - sum of a family of ideals: $\Sigma_{\lambda \in \Lambda} I_\lambda := (\bigcup_{\lambda \in \Lambda} I_\lambda)$;
  - $I_1 \cdots I_k := (\{i_1 \cdots i_k : i_j \in I_j\})$;
  - A power of an ideal $I^n := I \cdots I$;
  - Quotient ideal: $I_1 : I_2 := \{x \in R : xI_2 \subset I_1\}$.

Lemma 0.3.
- *The result of any of the above operations is an ideal.*
- *Show that the set $\{i_1 \cdots i_k : i_j \in I_j\}$ does not have to be an ideal.*
- *Show that $I_1 \cup I_2$ does not have to be an ideal.*

Remark 0.4. *In general $I_1 \cdots I_k \subsetneq I_1 \cap \dots \cap I_n$.*

2010 *Mathematics Subject Classification.* Primary:

An ideal is *finitely generated* if it is of the form $(i_1, \dots, i_k) = Ri_1 + \cdots + Ri_k$ for some elements $i_1, \dots, i_k \in R$.

Two important cases of quotient ideals are:

- the annihilator of an ideal J given by $\operatorname{ann}(J) := 0 : J$
- the annihilator of an element x given by $\operatorname{ann}(x) := 0 : (x)$.

Example 0.5. *If $R = \mathbb{Z}$ and $I = (m)$, $J = (n)$ then $I : J = (\frac{m}{\mathrm{GCD}(m,n)})$.*

Lemma 0.6. *Basic properties of operations on ideals are as follows:*

(i) $I \subset I : J$
(ii) $(I : J)J \subset I$
(iii) $(I : J) : L = I : (JL) = (I : L) : J$
(iv) $(\bigcap_\lambda I_\lambda) : J = \bigcap_\lambda (I_\lambda : J)$
(v) $D(R) = \bigcup_{x \neq 0} \operatorname{ann}(x)$

Definition 0.7 (Radical, Nilradical, Reduced ring, Reduction)**.** *For an ideal $I \lhd A$ we define its* radical *by*

$$\operatorname{rad}(I) := \{x \in A | \exists_{n \in \mathbb{Z}_+} x^n \in I\} \lhd A.$$

The nilradical *of a ring A is* $\operatorname{nil}(A) := \operatorname{rad}(0)$.
A ring A is reduced *if* $\operatorname{nil}(A) = 0$.
A reduction of a ring A is $A_{red} := A/\operatorname{nil}(A)$.

Definition 0.8 (Contraction, Extension)**.** *Let $f \colon A \to B$ a ring morphism. For an ideal $I \lhd A$ we define its* extension

$$I^e := (f(I)),$$

denoted also by IB. For an ideal J of B we define its contraction

$$J^c := f^{-1}(J),$$

denoted also $J \cap A$. In particular, $0^c = \ker f$.

Lemma 0.9. *(i) Contraction of an ideal is an ideal.*
(ii) An image of an ideal does not have to be an ideal.
(iii) $I \subset I^{ec}$, $J \supset J^{ce}$;
(iv) $I^e = I^{ece}$, $J^c = J^{cec}$.

Let $\mathcal{C} := \{J \cap A | J \lhd B\}$ be the set of ideals that are contractions of ideals in B and let $\mathcal{E} := \{IB | I \lhd A\}$ be the set of ideals that are extensions of ideals in A.

Lemma 0.10.
- *$\mathcal{C} = \{I \lhd A | I^{ec} = I\}$, $\mathcal{E} = \{J \lhd B | J^{ce} = J\}$;*
- *Extension and contraction give pairwise inverse bijections between $\mathcal{C}$ and $\mathcal{E}$;*
- *$\mathcal{C}$ is closed under taking interseciton and radical;*
- *$\mathcal{E}$ is closed under taking sum and product.*

For a morphism $f \colon A \to B$ we have:

- *$J \lhd B \Rightarrow \operatorname{rad}(J^c) = (\operatorname{rad} J)^c$;*
- *$I \lhd A$, f is an epimorphism, $\ker f \subset I$, then $\operatorname{rad}(I^e) = (\operatorname{rad}(I))^e$.*

A very important case is the canonical epimorphism:

$$\pi : A \to A/I,$$

for $I \lhd A$. Then for $I' \lhd A$ we have:

$$(I')^e = \pi(I') = (I + I')/I,$$
$$(I')^{ec} = \pi^{-1}(pi(I')) = I + I'.$$

The contraction map defines a bijection between ideals $J \lhd A/I$ and those ideals of A which contain I.

By Lemma **??** $\pi(\operatorname{rad} I) = \operatorname{nil}(A/I)$, so A_{red} is a reduced ring.

Lemma 0.11. *For two ideals $I, J \lhd A$ we have:*

(i) $I \subset \operatorname{rad}(I)$*;*
(ii) $\operatorname{rad}(\operatorname{rad}(I)) = \operatorname{rad}(I)$*;*
(iii) $\operatorname{rad} IJ = \operatorname{rad}(I \cap J) = (\operatorname{rad} I) \cap (\operatorname{rad} J)$*;*
(iv) $\operatorname{rad} I = (1) \Leftrightarrow I = (1)$*;*
(v) $\operatorname{rad}(I + J) = \operatorname{rad}(\operatorname{rad}(I) + \operatorname{rad}(J))$*;*
(vi) $\operatorname{rad}(I) + \operatorname{rad}(J) = (1) \Leftrightarrow I + J = (1)$*;*

Definition 0.12 (Maximal ideal, Maximal spectrum, Jacobson radical)**.** *An ideal $m \lhd A$ is called* maximal *if it is proper and for any $J \lhd A$ if $m \subset J \subset A$ then $m = J$ or $J = A$. In other words, it is maximal with respect to inclusion, among proper ideals.*

The set

$$\operatorname{Max}(A) := \{m \lhd A | m \text{ is maximal}\}$$

of maximal ideals is called the maximal spectrum*.*

The intersection of all maximal ideals

$$J(A) := \bigcap_{m \in \operatorname{Max}(A)} m$$

is called the Jacobson radical*.*

Proposition 0.13. *(i)* $m \in \operatorname{Max}(A) \Leftrightarrow A/m$ *is a field;*
(ii) Every proper ideal is contained in a maximal ideal. In particular, every element of $A \setminus U(A)$ is contained is a maximal ideal.
(iii) $\operatorname{Max}(A) \neq \emptyset$*;*
(iv) $x \in J(A) \Leftrightarrow \forall_{y \in A} 1 - xy \in U(A)$*.*

Proof. (i) Exercise.
(ii) A direct application of Zorn's lemma (known in Poland as Kuratowski-Zorn lemma).
(iii) $(0) \subset m \in \operatorname{Max}(A)$
(iv) $\Rightarrow$: $x \in J(A)$. Suppose $1 - xy \notin U(A)$ for some $y \in A$. Then there exists such $m \in \operatorname{Max}(A)$ that $1 - xy \in m$. As $x \in m$ this would imply that $1 \in m$ which is a contradiction.
$\Leftarrow$: Suppose for contradiction that for all $y \in A$ we have $1 - xy \in U(A)$ and there is a maximal ideal m that does not contain x. Then $(x) + m = (1)$, i.e. there exists $y_0 \in A$ such that $1 - xy_0 \in m$, hence $1 - xy_0 \notin U(A)$.

□

Definition 0.14 (Local and semilocal rings, Residue field)**.** *A ring A is called* local *if it has just one maximal ideal m. A local ring is usually represented as a pair (A, m) or a triple $(A, m, k = A/m)$ and the field k is called* the residue field*.*

A ring A is called semilocal *if $|\operatorname{Max}(A)| < \infty$.*

Proposition 0.15. *(i) If (A,m) is local then $U(A)=A\setminus m$.*
(ii) If $m\lhd A$, $m\neq A$ and $A\setminus m\subset U(A)$ then A is local and m is the maximal ideal.
(iii) If $m\in \operatorname{Max} A$ and $1+m\subset U(A)$ then A is local.

Proof. (i) Every proper ideal is disjoint from $U(A)$, so $m\subset A\setminus U(A)$. Every noninvertible element is contained in a maximal ideal, so $A\setminus U(A)\subset m$.
(ii) It follows that $A\setminus U(A)\subset m$, hence every proper ideal is contained in m.
(iii) If $x\in A\setminus m$ then $(x)+m=A$. Hence, there exist $y\in A$ and $b\in m$ such that $xy+b=1$. Hence, $xy\in U(A)$ and thus $x\in U(A)$.

□

Theorem 0.16 (Chinese Reminder Theorem)**.** *Let $I_1,\dots,I_r\lhd A$ be pairwise coprime ideals of A, i.e. $I_i+I_j=A$ for $i\neq j$. Then:*
(i) $I_1\cdots I_r=I_1\cap\cdots\cap I_r$. In particular, if A is semilocal then $J(A)$ is the product of maximal ideals.
(ii) $A/(I_1\cdots I_r)\simeq A/I_1\times\cdots\times A/I_r$.

Proof. (i) For $r=2$ we have:

$$I_1\cap I_2=(I_1+I_2)(I_1\cap I_2)\subset I_1(I_1\cap I_2)+I_2(I_1\cap I_2)\subset I_1I_2.$$

For $r>2$ let $J=I_1\cdots I_{r-1}=I_1\cap\cdots\cap I_{r-1}$. The claim follows by induction if we know that $J+I_r=A$. To show this, pick such $x_i\in I_i$, $y_i\in I_r$ for $i=1,\dots,r-1$ that $x_i+y_i=1$. Then $J\ni\prod_{i=1}^{r-1}x_i=\prod_{i=1}^{r-1}(1-y_i)$. This element is 1 modulo I_r.
(ii) Consider the morphism:

$$A\ni x\to(x+I_1,\dots,x+I_r)\in A/I_1\times\cdots\times A/I_r.$$

The kernel equals $I_1\cap\cdots\cap I_r$ which by point 1) equals $I_1\cdots I_r$. To finish the proof it remains to prove that the map is surjective.

For $r=2$ we pick such $x_1\in I_1$, $x_2\in I_2$ that $x_1+x_2=1$. Pick $(a+I_1,b+I_2)\in A/I_1\times A/I_2$. The element bx_1+ax_2 maps to the given one, as e.g. $bx_1+ax_2=ax_1+ax_2=a$ modulo I_1.

For $r>2$ the proof follows by induction, as in the previous point.

□

Mateusz Michałek,
`wajcha2@poczta.onet.pl`