LESSON 3 - REVIEW OF RING THEORY II

ERAN ASSAF

1. Introduction

Last lesson we reviewed the definitions of rings, homomorphisms and ideals, with a view towards polynomial rings, and defined integral domains and fields. Today, we are going to remind ourselves some properties of ideals and of integral domains.

2. properties of ideals

Definition 1. *Let I be an ideal of R. If there is $a \in R$ such that $I = aR$, we say that I is a* **principal ideal***.*

Example 2. *Every ideal in $\mathbb{Z}$ is principal. The ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal.*

Definition 3. *An ideal M in a ring R is a* **maximal ideal** *if $M \neq R$ and there isn't any ideal $M \subsetneq I \subsetneq R$.*

(Alternative description - if $M \subseteq I$ then either $I = M$ or $I = R$)

Example 4. *The ideals $p\mathbb{Z}$ in $\mathbb{Z}$ are maximal when p is prime.*

Proposition 5. *Every proper ideal is contained in a maximal ideal.*

Proof. Let I be a proper ideal in R. Let $\mathcal{S}$ be the set of all proper ideals of R which contain I. Then $I \in \mathcal{S}$, hence $\mathcal{S}$ is nonempty, and is partially ordered by inclusion. If $\mathcal{C}$ is a chain in $\mathcal{S}$, define $J_{\mathcal{C}} = \bigcup_{J \in \mathcal{C}} J$. Since $0 \in J$ for all $J \in \mathcal{C}$, we have $0 \in J_{\mathcal{C}}$. If $a, b \in J_{\mathcal{C}}$, there are $J_a, J_b \in \mathcal{C}$ such that $a \in J_a, b \in J_b$. Since either $J_a \subseteq J_b$ or $J_b \subseteq J_a$, we have $a - b \in J_{\mathcal{C}}$, showing it is a subgroup. Finally, if $a \in R$ and $x \in J_{\mathcal{C}}$, then $x \in J$ for some $J \in \mathcal{C}$ so $ax \in J \subseteq J_{\mathcal{C}}$, showing that $J_{\mathcal{C}}$ is an ideal. If $J_{\mathcal{C}}$ is not proper, then $1 \in J_{\mathcal{C}}$, hence $1 \in J$ for some $J \in \mathcal{C}$, contradiction. This proves that every chain has an upper bound in $\mathcal{S}$. By Zorn's lemma $\mathcal{S}$ has a maximal element which is a maximal ideal containing I. □

Proposition 6. *If R is commutative, an ideal M is maximal $\iff$ the quotient ring R/M is a field.*

Proof. If M is maximal, and $a \in R \setminus M$, then $M + aR = R$, so there exists $b \in R$ such that $1 - ab \in M$, so that $(a + M)(b + M) = 1 + M$, showing that R/M is a field. Conversely, if R/M is a field, and $M \subsetneq I$, there exists $a \in I \setminus M$ and some $b \in R$ such that $1 - ab \in M$, hence $1 \in aR + M \subseteq I$, showing that $I = R$. □

Corollary 7. *The quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field $\iff$ p is prime. We denote $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Example 8. *The ideal $(x) \subseteq \mathbb{Z}[x]$ is not maximal, as $(x) \subseteq (2,x) \subseteq \mathbb{Z}[x]$. The ideal $(2,x)$ is maximal, as $\mathbb{Z}[x]/(2,x) \simeq \mathbb{Z}/2\mathbb{Z}$ is a field.*

Definition 9. *An ideal P in a ring R is a* **prime ideal** *if for any $a,b \in R$ such that $ab \in P$, either $a \in P$ or $b \in P$.*

Example 10. *The ideal $(x) \subset \mathbb{Z}[x]$ is a prime ideal.*

Proposition 11. *If R is commutative, an ideal P is prime $\iff$ the quotient ring R/P is an integral domain.*

Proof. P is prime iff $ab \in P \implies a \in P$ or $b \in P$, which is equivalent to

$$(a+P)(b+P) = 0+P \implies a+P = 0+P \text{ or } b+P = 0+P,$$

which is the condition for R/P to be an integral domain. □

Corollary 12. *A maximal ideal is prime.*

Proof. Fields are integral domains. □

Corollary 13. *Let R be an integral domain, then either R has a subring isomorphic to $\mathbb{Z}$, in which case we say that R has* **characteristic** *0, or it has a subring isomorphic to $\mathbb{F}_p$ for some prime p, in which case we say that R has* **characteristic** *p.*

Proof. Consider the map $i_R : \mathbb{Z} \to R$. Then $\mathbb{Z}/\ker i_R \simeq i_R(\mathbb{Z})$ is a subring of R, hence an integral domain, so $\ker i_R$ is a prime ideal. Therefore, either $\ker i_R = 0$ or there is a prime p such that $\ker i_R = p\mathbb{Z}$. In the former case, i_R is injective, and embeds $\mathbb{Z} \simeq i_R(\mathbb{Z}) \subseteq R$ in R. In the latter, i_R induces an isomorphism

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \simeq i_R(\mathbb{Z}) \subseteq R. \quad \square$$

Corollary 14. *Let I be an ideal of R, and let $I[x]$ be the ideal of $R[x]$ generated by I. Then*

$$R[x]/I[x] \simeq (R/I)[x].$$

In particular, if I is a prime ideal of R, then $I[x]$ is a prime ideal of $R[x]$.

Proof. The natural projection $\pi : R \to R/I$ can be extended to a homomorphism $\widetilde{\pi} : R[x] \to (R/I)[x]$, with kernel $\ker \widetilde{\pi} = I[x]$. The first isomorphism theorem proves the first statement. For the second, if I is a prime ideal, R/I is an integral domain, hence so is $(R/I)[x] \simeq R[x]/I[x]$, so $I[x]$ is a prime ideal of $R[x]$. □

Example 15. *Let $R = \mathbb{Z}$ and consider the ideal $n\mathbb{Z}$ of $\mathbb{Z}$, then we obtain*

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \simeq \mathbb{Z}/n\mathbb{Z}[x],$$

and the natural projection map by reducing the coefficients modulo n is a ring homomorphism. If n is composite, the quotient ring is not an integral domain. If n is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field, and so $\mathbb{Z}/p\mathbb{Z}$ is an integral domain.

3. Euclidean Domains and PIDs

Definition 16. *Let R be an integral domain. A function $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ is called a* **norm** *on R. If $N(a) > 0$ for all a, N is a* **positive norm**.

Definition 17. *An integral domain R is a* **Euclidean Domain** *if there is a norm N on R such that for any $a, b \in R$ such that $b \neq 0$, there exist $q, r \in R$ such that*

$$a = qb + r, \quad r = 0 \text{ or } N(r) < N(b).$$

Example 18. *The integers $\mathbb{Z}$ are a Euclidean Domain, with $N(a) = |a|$.*

Proof. Division algorithm in $\mathbb{Z}$. □

Theorem 19. *If F is a field, then $F[x]$ is a Euclidean Domain with $N(p(x)) = \deg p(x)$. More precisely, if $a(x), b(x) \in F[x]$, with $b(x) \neq 0$ there are unique $q(x), r(x) \in F[x]$ such that*

$$a(x) = q(x)b(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg b(x).$$

Proof. We start with proving existence. If $a(x) = 0$, set $q(x) = r(x) = 0$. Assume $a(x) \neq 0$, and prove by induction on $n = \deg a(x)$. Let $m = \deg b(x)$. If $n < m$, take $q(x) = 0$ and $r(x) = a(x)$. Otherwise $n \geq m$. Note that if $n = 0$, then also $m = 0$, and $a = a(x), b = b(x) \in F^{\times}$ so we may take $q(x) = ab^{-1}, r(x) = 0$. Write

$$a(x) = a_n x^n + \ldots + a_1 x + a_0, \quad b(x) = b_m x^m + \ldots + b_1 x + b_0,$$

and consider the polynomial (note $b_m \neq 0$ is invertible, since F is a field)

$$c(x) = a(x) - b_m^{-1} a_n x^{n-m} b(x).$$

Then $\deg c(x) < n$. By induction, there are $p(x), r(x)$ with

$$c(x) = p(x)b(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg b(x).$$

Then we can write $q(x) = p(x) + b_m^{-1} a_n x^{n-m}$ and get

$$a(x) = q(x)b(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg b(x).$$

For uniqueness, suppose $q_1(x), r_1(x)$ also satisfy the conditions. Then

$$r(x) - r_1(x) = (a(x) - q(x)b(x)) - (a(x) - q_1(x)b(x)) = b(x)(q(x) - q_1(x)).$$

If $q(x) - q_1(x) \neq 0$, then it follows that

$$\deg(r(x) - r_1(x)) = \deg b(x) + \deg(q(x) - q_1(x)) \geq \deg b(x),$$

contradiction. Therefore $q(x) = q_1(x)$ and $r(x) = r_1(x)$. □

Definition 20. *A* **Principal Ideal Domain** *is an integral domain in which every ideal is principal.*

Example 21. *The integers $\mathbb{Z}$ form a PID.*

Example 22. *The polynomial ring over the integers $\mathbb{Z}[x]$ is not a PID.*

Proposition 23. *Every Euclidean Domain R is a PID.*

Proof. Let $0 \neq I \subseteq R$, and let $0 \neq b \in I$ have minimal norm. If $a \in I$, then $a = qb + r$ for some $q, r \in R$ with $N(r) < N(b)$ or $r = 0$. By minimality of b, we must have $r = 0$ hence $a \in (b)$. It follows that $I = (b)$ is principal. □

Proposition 24. *Every nonzero prime ideal P in a PID R is maximal.*

Proof. Write $P = (p) \subseteq (a)$. Then $p = ab$ for some $b \in R$. Since P is prime, either $a \in P$ or $b \in P$. If $a \in P$, then $(a) = P$. If $b \in P$, then $b = pu$ for some $u \in R$, hence $1 = au \in (a)$. Therefore $(a) = R$. Thus, P is maximal. □

4. summary

Today we recalled some properties of ideals and properties of some integral domains, and that quotient rings are fields for maximal ideals and integral domains for prime ideals. We have seen that any integral domain, and in particular any field, has a characteristic, which is either 0 or a prime p. We proved that the polynomials over a field form a Euclidean domain, hence a PID.

5. Appendix: on Zorn's Lemma

During the lesson it became clear that not everyone is familiar with Zorn's Lemma. As this is an important tool in mathematics, I provide a brief review of it here. The interested reader can of course read about it in the literature.

The idea behind Zorn's lemma is to allow one use the axiom of choice to prove existence of maximal objects in uncountable situations. This allows one to apply al the machinery of transfinite induction only implicitly.

Since Zorn's lemma is a very general statement, we will take a step back and consider general partially ordered sets. Before stating the lemma, let us define a few concepts related to them. We begin by defining a partially ordered set.

Definition 25. *Let S be a set. Let $2^S = \{T : T \subseteq S\}$ be the set of subsets of S. It is called the* **power set** *of S.*

Definition 26. *Let S be a set. A* **relation** *R on S is a subset $R \subseteq S \times S$. For elements $x, y \in S$, we denote by xRy the statement $(x, y) \in R$.*

A relation is sometimes called a binary relation, or a homogeneous relation.

Example 27. *The relation $\leq$ on $\mathbb{Z}$ is given by $" \leq " = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \leq b\}$. Similarly $\geq, <, >, =, \neq, |$ are relations on $\mathbb{Z}$.*

Definition 28. *Let P be a set and $\leq$ a relation on P. Then $\leq$ is a* **partial order** *on P if it satisfies the following three properties.*

(1) **Reflexivity** *: $x \leq x$ for all $x \in P$.*
(2) **Antisymmetry** *: If $x \leq y$ and $y \leq x$, then $x = y$ for all $x, y \in P$.*
(3) **transitivity** *: If $x \leq y$ and $y \leq z$, then $x \leq z$ for all $x, y, z \in P$.*

The pair $(P, \leq)$ is called a **partially ordered set**.

Example 29. *The relation $\leq$ on $\mathbb{Z}$ is a partial order.*

Example 30. *Let S be a set. The relation $\subseteq$ on its power set 2^S is a partial order.*

In some circumstances, we can't compare all elements in our poset, but when we can it is usually much easier to work with. Therefore sets in which we can compare any two objects deserve special attention.

Definition 31. *A partially ordered set $(P, \leq)$ is a* **totally ordered set** *if for any $x, y \in P$ either $x \leq y$ or $y \leq x$. If $(P, \leq)$ is a partially ordered set and $C \subseteq P$ is such that $(C, \leq)$ is totally ordered, we say that C is a* **chain** *in P.*

Example 32. *The set $\mathbb{Z}_{\geq 1}$ is partially ordered together with the division relation $a \mid b$, but it is not totally ordered. A chain in $(\mathbb{Z}_{\geq 1}, |)$ is a sequence of integers $\{a_n\}_{n=1}^{\infty}$ such that $a_n \mid a_{n+1}$ for all n.*

Example 33. $(\mathbb{R}, \leq)$ *is a totally ordered set. In particular $\mathbb{R}$ is an uncountable chain in $\mathbb{R}$, showing that chains need not be countable.*

Finally, we want to introduce notion of bounds and maximality, to actually be able to find a maximal element.

Definition 34. *Let $(P, \leq)$ be a partially ordered set, and let $S \subseteq P$ be a subset. An element $x inP$ such that $s \leq x$ for all $s \in S$ is an* **upper bound** *for S in P.*

Example 35. *In $(\mathbb{Z}_{\geq 1}, |)$, if $S = \{a_1, \ldots, a_n\} \subseteq \mathbb{Z}_{\geq 1}$ is finite, then the element* $\operatorname{lcm}(S) = \operatorname{lcm}(a_1, \ldots, a_n)$ *is an upper bound for S in $\mathbb{Z}_{\geq 1}$.*

Definition 36. *Let $(P, \leq)$ be a partially ordered set. A* **maximal element** *$x \in P$ is an element such that for all $y \in P$, $x \leq y \implies x = y$.*

Example 37. *The set $S = \{x \in \mathbb{Q} \mid x \leq \sqrt{2}\} \subseteq \mathbb{Q}$ is a chain in $(\mathbb{Q}, \leq)$ that has no maximal element. Any rational number larger than $\sqrt{2}$ will be an upper bound for S in $\mathbb{Q}$.*

We now have all the definitions in place to formulate Zorn's Lemma.

Lemma 38 (Zorn's Lemma)**.** *Let $(P, \leq)$ be a partially ordered set. Assume that every chain in P has an upper bound in P. Then P contains a maximal element.*

It is sometimes simpler and more common to use the following equivalent formulation.

Lemma 39 (Zorn's Lemma)**.** *Let $(P, \leq)$ be a nonempty partially ordered set. Assume that every nonempty chain in P has an upper bound in P. Then P contains a maximal element.*

Proof Sketch. Suppose on the contrary that the lemma is false. Then there exists a poset P such that every chain $C \subseteq P$ has an upper bound, and P does not contain any maximal element. For any $C \subseteq P$, let $u(C) \in P$ be its upper bound. Since $u(C)$ is not maximal, there exists an element $b(C) \in P$ such that $u(C) < b(C)$. Note that by the axiom of choice, we can define such a function b.

We use the function b to obtain a contradiction. Since P is nonempty, it contains an element $a_0 \in P$. Assume by (transfinite) induction that we have constructed all elements a_α with $\alpha < \omega$. Then we define $a_\omega = b(\{a_\alpha : \alpha < \omega\})$. In particular, if we choose a cardinal $\omega > |P|$, we construct a subset of $|P|$ of size ω, a contradiction. □