2. Introduction to commutative rings (continued)

2.1. **New examples of commutative rings.** Recall that in the first lecture we defined the notions of commutative rings and field and gave some examples of those. All the examples we discussed last time were already known to us (mostly from high school), so we did not really establish anything new by stating that those were commutative rings/fields (we simply rephrased what we already knew in a new language). In this lecture we will describe two essentially new examples of commutative rings with 1 where, in particular, we will need to define + and · (rather than use operations that we are already familiar with).

Example 2.1. Let X be any set, and let $R = \mathcal{P}(X)$, the set of all subsets of X (also known as the *power set* of X). For instance, if X is the two element set $\{0, 1\}$, then R has 4 elements: $\{0\}$, $\{1\}$, $\emptyset$ (the empty set) and $\{0, 1\} = X$.

Define binary operations + and · on R by

$$A \cdot B = A \cap B \text{ (the intersection of } A \text{ and } B) \text{ and}$$
$$A + B = (A \cup B) \setminus (A \cap B).$$

The set $(A \cup B) \setminus (A \cap B)$ is called the *symmetric difference* of A and B. This name is justified by the equality $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$ (which is straightforward to check). In logic, the operation that produces $(A \cup B) \setminus (A \cap B)$ from A and B is called the 'exclusive or'. This terminology is also clear since $(A \cup B) \setminus (A \cap B)$ is the set of elements which lie in A or in B but not in both.

We claim that R with these operations is a commutative ring with 1, that is, satisfies axioms (A0)-(A4), (M0)-(M3) and (D1)-(D2). In class we will check multiplication axioms (M0)-(M3); the rest will be left as a homework problem.

(M0) This simply says that if A, B are subsets of X, then $A \cap B$ is also a subset of X, which is clearly true.

(M1) asserts that $A \cap B = B \cap A$ for all $A, B \subseteq X$. This is also clear.

(M2) asserts that $A \cap (B \cap C) = (A \cap B) \cap C$ for all $A, B, C \subseteq X$. This is also a property you are probably familiar with, but it is not nearly as obvious as (M1), so let us prove it.

A standard technique for proving that two sets are equal is to show that they are contained in each other. Verifications of inclusions $A \cap (B \cap C) \subseteq$

$(A \cap B) \cap C$ and $(A \cap B) \cap C \subseteq A \cap (B \cap C)$ are very similar, so we will only do the first one.

To prove that $A \cap (B \cap C) \subseteq (A \cap B) \cap C$ we need to show that any $x \in A \cap (B \cap C)$ is also an element of $(A \cap B) \cap C$. So take any $x \in A \cap (B \cap C)$. Then, by definition of the intersection, $x \in A$ and $x \in B \cap C$, whence $x \in A$ and $x \in B$ and $x \in C$. The first two conditions imply that $x \in A \cap B$. Thus, $x \in A \cap B$ and $x \in C$, whence $x \in (A \cap B) \cap C$. Thus, we showed that $A \cap (B \cap C) \subseteq (A \cap B) \cap C$.

Finally, to check (M3) we need to show that there exists a subset of X (which we denote by symbol 1) such that $1 \cap A = A$ for all $A \subseteq X$. Clearly, this property holds if we set $1 = X$.

Example 2.2. *Let $n \geq 2$ be an integer, and let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \{x \in \mathbb{Z} : 0 \leq x \leq n-1\}$. We want to define addition and multiplication on $\mathbb{Z}_n$ which will turn it in a commutative ring with 1.*

First of all note that we cannot use the usual addition and multiplication since $\mathbb{Z}_n$ is not closed under those. We shall denote the addition and multiplication we will be defining by symbols $\oplus$ and $\odot$ (to avoid confusion with the usual addition and multiplication). To make our task more specific we will impose an extra requirement on the operations $\oplus$ and $\odot$ we are trying to define:

(*) $x \oplus y = x + y$ whenever $0 \leq x + y \leq n - 1$ and $x \odot y = xy$ whenever $0 \leq xy \leq n - 1$ (where the sum and the product on the right-hand sides are the usual addition and multiplication).

Informally, condition (*) means that we want the newly defined operations $\oplus$ and $\odot$ to be as close to $+$ and $\cdot$ as possible.

So, the precise question we are trying to answer is the following:

Question 2.3. *Can we define operations $\oplus$ and $\odot$ on $\mathbb{Z}_n$ such that $\mathbb{Z}_n$ with those operations is a commutative ring with 1 and, in addition, condition (*) holds. If yes, is there a unique way to do it?*

It turns out that the answer to both parts of this question is positive. Today we will address the uniqueness part, that is, we will try to show that if we want $\oplus$ and $\odot$ to satisfy all of the above conditions, then at least we do not have any choice. In class we will consider this problem for $n = 3$, and in the homework you will be asked to do the same for $n = 4$ and 5 (once you do the cases $n = 4, 5$, try to extend the argument to arbitrary n).

So, let $n = 3$, and let us start with addition $\oplus$. By (*) we are already "committed" to having equalities $0 \oplus x = x \oplus 0 = x$ for all x and $1 \oplus 1 = 2$, so the only remaining questions are what is $1 \oplus 2$ and what is $2 \oplus 2$ (since we want (A1) to hold, we must have $1 \oplus 2 = 2 \oplus 1$).

We claim that $1 \oplus 2 = 0$. We argue that any other choice for $1 \oplus 2$ immediately leads to a contradiction. Indeed, if $1 \oplus 2 \neq 0$, then $1 \oplus 2 = 1$ or $1 \oplus 2 = 2$. But if $1 \oplus 2 = 1$, then $1 \oplus 2 = 1 \oplus 0$, so by the additive cancellation law (which, as we showed last time, holds in any ring), we get $2 = 0$, which is impossible since by our setup 0 and 2 are different elements of $\mathbb{Z}_3$. Similarly, $1 \oplus 2 = 2$ would imply $1 = 0$, which again is impossible.

So, we must have $1 \oplus 2 = 2 \oplus 1 = 0$. Similar argument shows that the only possible choice for $2 \oplus 2$ is $2 \oplus 2 = 1$. Thus, we completed the addition table:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

For multiplication table we already know that we must have $0 \odot x = x \odot 0 = 0$ for all x, $1 \odot x = x \odot 1 = x$ for all x, so the only question is what is $2 \odot 2$. To determine this, we use the distributivity axiom: $2 \odot 2 = (1 \oplus 1) \odot 2 = 1 \odot 2 \oplus 1 \odot 2 = 2 \oplus 2 = 1$, so the multiplication table is completed as well:

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

So, what did we accomplish? We showed that if there is any way to define $\oplus$ and $\odot$ on $\mathbb{Z}_3$ such that axioms of a commutative ring with 1 and condition (*) all hold, then $\oplus$ and $\odot$ must be defined by the above tables. We still do not know if $\oplus$ and $\odot$ defined as above will satisfy these conditions – this turns out to be true, but so far we do not have tools to prove it in a nice way (we will get back to this problem in Lecture 8).

However, if for now we assume without proof that $\mathbb{Z}_3$ with the above operations is indeed a commutative ring with 1, then we can already answer some questions about it. For instance, we can determine whether $\mathbb{Z}_3$ is a filed directly from the multiplication table. Indeed, we have $1 \cdot 1 = 1$ and $2 \cdot 2 = 1$, so both 1 and 2 are invertible ($1^{-1} = 1$ and $2^{-1} = 2$). Thus, all nonzero elements of $\mathbb{Z}_3$ have a multiplicative inverse, so $\mathbb{Z}_3$ is indeed a field.

2.2. **Inequalities and ordered rings.** In the last lecture we formalized what we mean by 'standard properties of arithmetic operations' in the form of axioms and define commutative rings and fields in terms of those axioms. Today we will do the same with inequalities. Again, we start with an idea for the definition.

Very informally speaking, an ordered ring is a ring in which we can talk about positive/negative elements and inequalities so that the usual properties holds. Based on this description, we would expect that $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ (with inequalities defined in the usual way) are ordered rings. We now give a formal definition

Definition. Let R be a ring. We say that R is an *ordered ring* if R has a distinguished subset $R_{>0}$ (called the subset of positive elements) satisfying the following three axioms:

(O1) For every $x \in R$ **exactly** one of the following three conditions is true: $x \in R_{>0}$, $-x \in R_{>0}$ or $x = 0$

(O2) If $x \in R_{>0}$ and $y \in R_{>0}$, then $x + y \in R_{>0}$ (the sum of two positive elements is positive)

(O3) If $x \in R_{>0}$ and $y \in R_{>0}$, then $xy \in R_{>0}$ (the product of two positive elements is positive)

Remark: In class we used the notation R_+ instead of $R_{>0}$.

Note that the above axioms only refer to positive elements and not to inequalities, but we can define inequalities in terms of positive elements. Given an ordered ring R and $x, y \in R$, we define $x > y \iff x - y \in R_{>0}$ and $x < y \iff y > x$ (thus, $x < y \iff y - x \in R_{>0}$).

All the standard properties of inequalities can be deduced from axioms (O1)-(O3). Below we show how to establish the transitivity property.

Example 2.4. Let R be an ordered ring. Then the relation $>$ is transitive, that is, if $x > y$ and $y > z$ for some $x, y, z \in R$, then $x > z$.

Proof. We need to express the given inequalities $x > y$ and $y > z$ in terms of positive elements, so that we can use the axioms. By definition, $x > y$ implies that $x - y \in R_{>0}$ and $y > z$ implies that $y - z \in R_{>0}$. By (02) we have $(x - y) + (y - z) \in R_{>0}$. Since $(x - y) + (y - z) = x - z$ (this identity follows from ring axioms similarly to other properties we verified in Lecture 1), we conclude that $x - z \in R_{>0}$, so again by definition $x > z$. □

2.3. **Book references.** The material from 2.1 is not really covered in either book. The ring in Example 2.1 appears in the exercises after Ch.17 in Pinter,

but not much is proved about it; as we will see in a couple of weeks, the ring $\mathbb{Z}_n$ from Example 2.2 is fundamental, so both Pinter and Gilbert (as well as any abstract algebra book) cover it in detail, but they do not mention the approach to constructing $\mathbb{Z}_n$ taken in this lecture.

The material from 2.2 is covered in the second part of 2.1 in Gilbert and 21.1 in Pinter, although the definition in Pinter's book looks very different from the one given in this lecture.