Lecture 6: Rings

Rajat Mittal ⋆

IIT Kanpur

We have shown that $\mathbb{Z}_n$ is a group under addition and $\mathbb{Z}_n^+$ is a group under multiplication (set of all numbers co-prime to n in $\mathbb{Z}_n$). Till now, the two operations $+$ and $\times$ have been treated differently. But from our experience with integers and even matrices, these operations satisfy properties like "distribution" $(a(b+c) = ab + ac)$.

Hence, after success in defining an abstract structure with one operation (group), now we define another abstract structure with 2 operations. The first question is, what should be the defining properties of this new abstract structure. We will be inspired by integers again and define the concept of *Rings*.

1 Rings

Consider two operations $+$ and $\times$ in a set R.

Definition 1. *The set R with the two operations $+$ and $\times$ is a* ring*, if,*

- *R is a commutative group under $+$.*
- *R is associative, closed and has an identity with respect to the operation $\times$.*
- *The two operations $+$ and $\times$ follow the distributive law, i.e.,*

$$a \times (b+c) = a \times b + a \times c \text{ and } (a+b) \times c = a \times c + b \times c.$$

Note 1. We will always assume that the multiplicative identity is different from additive identity. The additive identity will be denoted by 0 and multiplicative identity by 1. For brevity, we will denote $a \times b$ as ab.

Exercise 1. Are the two conditions under the distributive law same?

Exercise 2. Why did we assume commutativity under addition for a ring?

There are many examples of rings, many of these sets we have encountered before.

- The sets $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$,$\mathbb{C}$ are rings with addition and multiplication.
- The set of integers modulo m, $\mathbb{Z}_m$, is a ring with addition and multiplication.
- The set of 2×2 matrices with integer entries is a ring. Actually if R is a ring then set of 2×2 matrices with entries in R is also a ring.

Another ring which will be of our particular interest is the ring of polynomials. The set $R[x]$ is the set of all polynomials with coefficients from ring R. If the multiplication in R is commutative then $R[x]$ is also a commutative ring.

Note 2. The addition and multiplication of polynomials is defined in the same way as in regular polynomials.

Exercise 3. Check that you can define these operations on polynomials with entries from a ring R. Why do we need that multiplication is commutative in the original ring?

Hence we have polynomial rings $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ having commutative multiplication.

⋆ Thanks to the book from Dummit and Foote and the book from Norman Biggs.

1.1 Units of a ring

The ring is not a group with respect to multiplication. That is because inverses need not exist in a ring (e.g., integers). The elements of rings which have inverses inside the ring with respect to multiplication are called *units* or *invertible elements*.

The set of units for $\mathbb{Z}$ are just ± 1.

Exercise 4. Prove that the set of units form a group under multiplication.

1.2 Characteristic of a ring

Rings have two identities $e_\times$ and e_+ (we will denote them by 1 and 0 respectively). For a ring an important criteria is the additive group generated by 1. The elements of that group are 1, $1+1$, $1+1+1$ and so on. The smallest number of times we need to sum 1 to get 0 is called the *characteristic* of the ring.

For some cases, like reals, the sum never reaches the additive identity 0. In these cases we say that the characteristic is *zero*.

Exercise 5. Prove that $1 \times 0 = 0$ in a ring.

1.3 Homomorphism for a ring

We have already defined the homomorphism for a group. How should we define the homomorphism for a ring?

Exercise 6. Try to come up with a definition of ring homomorphism. Remember that the mapping should be well behaved with respect to both the operators.

When not clear from the context, we specify if it is a group homomorphism or a ring isomorphism.

We can define the *kernel* of a homomorphism $\phi : R \to S$ from a ring R to ring S as the set of elements of R which map to the additive identity 0 of S. A bijective homomorphism is called an isomorphism.

We showed in previous lectures that the kernel of a group homomorphism is a normal subgroup. What about the kernel of a ring homomorphism? For this, the concept of ideals will be defined.

1.4 Ideal

The ring R is a group under addition. A subgroup I of R under addition is called an *ideal* if

$$\forall x \in I, r \in R : \quad xr, rx \in I$$

For example, the set of all elements divisible by n is an ideal in $\mathbb{Z}$.

Exercise 7. Show that $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Ideal is similar to the normal subgroup, but belongs to a ring. Suppose I is an ideal. Then we can define the set of cosets of I with respect to R as $\frac{R}{I}$. We denote the elements of the set by $r + I$.

We know that $\frac{R}{I}$ is a group (why?), but it can be shown that it is a ring under the following operations too.

$$(r+I) + (S+I) = (r+s) + I \quad (r+I) \times (s+I) = (rs) + I$$

Exercise 8. Show that the kernel of a ring homomorphism is an ideal.

Kernel of a any ring homomorphism is an ideal and every ideal can be viewed this way. We can define quotient ring using ideals as we defined quotient group using normal subgroup. It turns out,

Theorem 1. *Given a homomorphism $\phi : R \to S$,*

$$\frac{R}{Ker(\phi)} \cong Img(\phi)$$

Given a set $S \subseteq I$, we can always come up with the ideal generated by the set. Suppose the multiplication is commutative, then

$$I = \{r_1x_1 + r_2x_2 + \cdots + r_nx_n : \ \forall i \ \ r_i \in R, x_i \in S\},$$

is the ideal generated by S.

Exercise 9. Prove that it is an ideal.

2 Chinese remainder theorem

One of the most important ways to create a big ring using two small rings is called *direct product*. Suppose the two given rings are R and S. The direct product $T = R \times S$ is a ring with first element from R and second element from S.

$$T = \{(r, s) : \quad r \in R \text{ and } s \in S\}$$

The two binary operations in ring T are defined by taking the operations component-wise in R and S.

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ and } (r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$$

The motivation for *Chinese remainder theorem* is to break the ring $\mathbb{Z}_m$ into smaller parts (rings modulo smaller numbers).

Exercise 10. Come up with an isomorphism between $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$.

It might seem that we can break $\mathbb{Z}_{mn}$ to $\mathbb{Z}_m \times \mathbb{Z}_n$.

Exercise 11. Show that there is no isomorphism between $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

It turns out, in the last exercise, 2 and 3 being co-prime to each other is important. We need to define when two ideals are "co-prime" to each other.

Definition 2. *The ideals A and B are said to be comaximal if $A + B = R$. Here $A + B = \{a + b : \ a \in A$ and $b \in B\}$.*

The definition of comaximal basically says that there exist $x \in A$ and $y \in B$, s.t., $x + y = 1$.

Note 3. Similarly we can define AB to be the ideal with *finite sums* of kind ab where $a \in A$ and $b \in B$.

Exercise 12. Notice that $S = \{ab : a \in A, b \in B\}$ need not be an ideal. Show that AB as defined above is an ideal.

Exercise 13. If $A_1, A_2, \cdots, A_k$ are pairwise comaximal then show that A_1 and $A_2 \cdots A_k$ are comaximal too.

With all these definitions (direct product, comaximal) we are ready to state the Chinese remaindering theorem. We will assume that the ring is commutative.

Theorem 2. *Chinese remainder theorem (CRT): Let $A_1, A_2, \cdots, A_k$ be ideals in ring R. The natural map which takes $r \in R$ to $(r + A_1, r + A_2, \cdots, r + A_k) \in \frac{R}{A_1} \times \frac{R}{A_2} \times \cdots \times \frac{R}{A_k}$ is a ring homomorphism. If all pairs A_i, A_j are comaximal then the homomorphism is actually surjective (onto) and,*

$$\frac{R}{A_1A_2 \cdots A_k} \cong \frac{R}{A_1} \times \frac{R}{A_2} \times \cdots \times \frac{R}{A_k}.$$

Proof. We will first show this for $k = 2$ and then it can be extended by induction (the exercise that A_1 and $A_2 \cdots A_k$ are comaximal will prove it).

The proof can be broken down into three parts.

1. The map ϕ which takes r to $r + A_1, r + A_2$ is a homomorphism.
2. The kernel ϕ is $A_1 A_2 \cdots A_k$.
3. The image is $\frac{R}{A_1} \times \frac{R}{A_2} \times \cdots \times \frac{R}{A_k}$. In other words the map ϕ is onto(surjective).

The first part is an exercise. It follows from the fact that the individual maps ($\delta_i : R \to \frac{R}{A_i}$) which take r to $r + A_i$ are homomorphisms.

The kernel for this individual maps are A_i's and hence for the combined map ϕ, it is $A_1 \cap A_2$. The second part of the proof requires us to prove that if A_1, A_2 are comaximal then $A_1 \cap A_2 = A_1 A_2$.

Suppose A_1 and A_2 are comaximal. Hence, there exist $x \in A_1, y \in A_2$ for which $x + y = 1$. Even without the comaximal condition $A_1 A_2 \subseteq A_1 \cap A_2$. For the opposite direction, say $c \in A_1 \cap A_2$, then $c = c1 = cx + cy \in A_1 A_2$ (there exist $x \in A_1, y \in A_2$ for which $x + y = 1$). Hence $A_1 \cap A_2 = A_1 A_2$.

Now we only need to prove the third part, to show that the map $\phi : r \to (r + A_1, r + A_2)$ is surjective. Since $x + y = 1$, $\phi(x) = (0, 1)$ and $\phi(y) = (1, 0)$. For any element $(r_1 + A_1, r_2 + A_2)$ of $\frac{R}{A_1} \times \frac{R}{A_2}$, we can prove $\phi(r_2 x + r_1 y) = (r_1 + A_1, r_2 + A_2)$. Hence ϕ is surjective.

$$\phi(r_2 x + r_1 y) = \phi(r_2 x) + \phi(r_1 y) = (A_1, r_2 + A_2) + (r_1 + A_1, A_2) = (r_1 + A_1, r_2 + A_2).$$

□

We will see various applications of Chinese remaindering theorem throughout this course. The most important one is, given a number $n = p_1^{a_1} \cdots p_r^{a_r}$,

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \mathbb{Z}_{p_2^{a_2}} \cdots \mathbb{Z}_{p_r^{a_r}}.$$

The proof is left as an exercise.

This isomorphism and its proof will enable us to answer one of the questions posted earlier. Suppose we need to find a number r which leaves remainder r_1 modulo n_1 and remainder r_2 modulo n_2. Chinese remainder theorem tells us that such a r *always exists* if n_1 and n_2 are co-prime to each other. Through the proof of CRT,

$$r = r_1 n_2 (n_2^{-1} \mod n_1) + r_2 n_1 (n_1^{-1} \mod n_2).$$

Exercise 14. Check that the above solution works.

The same can be generalized to more than 2 numbers. How (try to give the explicit formula)?

Now, we will consider two abstract structures which are specialization of rings, integral domains and fields.

3 Integral domain

Our main motivation was to study integers. We know that integers are rings but they are not fields. We also saw (through exercise) that integers are more special than rings. The next abstract structure is very close to integers and is called *integral domain*.

An *integral domain* is a commutative ring (multiplication is commutative) where product of two non-zero elements is also non-zero. In other words, if $ab = 0$ then either $a = 0$ or $b = 0$ or both.

Exercise 15. Give some examples of an integral domain. Give some examples of rings which are not integral domains.

We said that integral domain is closer to integers than rings. The first thing to notice is that integral domains have cancellation property.

Exercise 16. If $ab = ac$ in an integral domain, then either $a = 0$ or $b = c$.

Now we will see that the properties of divisibility, primes etc. can be defined for integral domains.

Given two elements $a, b \in R$, we say that a *divides* b (b is a *multiple* of a) if there exist an $x \in R$, s.t., $ax = b$.

Exercise 17. If a divides b and b divides a then they are called *associates*. Show,

- Being associates is an equivalence relation.
- a and b are associates iff $a = ub$ where u is a unit.

You can guess (from the example of integers), the numbers 0 and units (± 1) are not relevant for divisibility. A non-zero non-unit x is *irreducible* if it can't be expressed as a product of two non-zero non-units. A non-zero non-unit x is *prime* if whenever x divides ab, it divides either a or b.

Notice that for integers the definition of irreducible and prime is the same. But this need not be true in general for integral domain. For examples, look at any standard text.

Exercise 18. What is the problem with defining divisibility in ring?

4 Fields

If you look at the definition of rings, it seems we were a bit unfair towards *multiplication*. R was a commutative group under addition but for multiplication the properties were very relaxed (no inverses, no commutativity). *Field* is the abstract structure where the set is *almost* a commutative group under multiplication.

Definition 3. *The set F with the two operations $+$ and $\times$ is a* field*, if,*

- *F is a commutative group under $+$.*
- *$F - \{0\}$ is a commutative group under $\times$ (it has inverses).*
- *The two operations $+$ and $\times$ follow the distributive law, i.e.,*

$$a \times (b + c) = a \times b + a \times c \text{ and } (a + b) \times c = a \times c + b \times c.$$

Exercise 19. Why are we excluding the identity of addition when the multiplicative group is defined?

As you can see Field has the strongest structure (most properties) among the things (groups, rings etc..) we have studied. Hence many theorems can be proven using Fields. Fields is one of the most important abstract structure for computer scientists.

Note 4. The notion of divisibility etc. are trivial in fields.

Let us look at some of the examples of fields.

- $\mathbb{Z}$ is NOT a field.
- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.
- $\mathbb{Z}_m$ is a field iff m is a _____. Ex: Fill in the blank.

The last example is of fields which have finite size. These fields are called *finite fields* and will be of great interest to us.

5 The chain of abstract structures (advanced)

We have studied three different abstract structures this week, ring, integral domain and fields. Actually there are a lot of abstract structures which can arise in between rings and fields. They are defined by the properties which have been fundamental in the study of number theory. Take a look at the definition of all of these structures and the relation (order) between the properties.

Exercise 20. For how many of them can you guess the defining properties?

Rings $\supset$ Commutative Rings $\supset$ Integral domain $\supset$ Unique factorization domain $\supset$ Principal ideal domain $\supset$ Euclidean domain $\supset$ Field

This list is taken from Wikipedia. You can interpret this chain of inclusion as the fact that Euclidean gcd algorithm (Euclidean domain) implies the every any number of the form $ax+by$ can be written as $dgcd(x,y)$ (principal ideal domain). And principal ideal domain implies unique factorization. Then unique factorization implies, $ab = ac \;\Rightarrow\; b = c$ assuming $a \neq 0$.

Exercise 21. Prove all the above assertions.

6 Assignment

Exercise 22. Give a rule that is satisfied by Integers but need not be satisfied by rings in general.

Exercise 23. Find the set of units in the ring $\mathbb{Z}_8$.

Exercise 24. If all the ideals in the ring can be generated by a single element then it is called a *principal ideal domain*. Show that $\mathbb{Z}$ is a principal ideal domain.

Exercise 25. Show that if $ab = 0$ for a, b in a field F then show that either $a = 0$ or $b = 0$.

Exercise 26. What are the units of a field?

Exercise 27. Show that a finite integral domain is a field.

Exercise 28. Show that the characteristic of a finite field is always a prime.

Exercise 29. Find a number n which leaves remainder 23 with 31, 2 with 37 and 61 with 73.

Exercise 30. Given a number $n = p_1^{a_1} \cdots p_r^{a_r}$, show that,

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \mathbb{Z}_{p_2^{a_2}} \cdots \mathbb{Z}_{p_r^{a_r}}.$$

Where $\cong$ denotes that two rings are isomorphic.

Exercise 31. Find a number n which leaves remainder 3 when divided by 33 and 62 when divided by 81.

Hint: Trick question.

Exercise 32. Suppose $\phi(n)$ is the number of elements co-prime to n. Prove that if m and n are co-prime, then $\phi(mn) = \phi(m)\phi(n)$.

Hint: Chinese remainder theorem.

Exercise 33. Show that $m\mathbb{Z}$ and $n\mathbb{Z}$ are comaximal in $\mathbb{Z}$.