Rajat Mittal *

Lecture notes: Abstract algebra

April 20, 2015

Springer

* Thanks to the book from Dummit and Foote and the book from Norman Biggs.
IIT Kanpur

1

Introduction

Please look at the course policies mentioned in the course homepage. Most importantly, any immoral behavior like cheating and fraud will be punished with extreme measures and without any exception.

1.1 What is this course about?

Take a look at the following questions.

- Give a number n which leaves a remainder of 20 when divided by 23 and 62 when divided by 83.

- How many different necklaces can you form with 2 black beads and 8 white beads? How many necklaces can you form with blue, green and black beads?
- What are the last two digits of of a^{40} when a is not divisible by 2 or 5?

- We know that there is an explicit formula for the roots of quadratic equation $ax^2+bx+c=0$, $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. Similarly there are explicit formulas for degree 3 and degree 4 equations. Why don't we have something for degree 5?
- When does the equations of the form $x-y=z$ make sense? If x is a natural number or an integer or a matrix or an apple or a permutation?

When we look at these questions, they seem unrelated and seem to have no common thread. Mathematicians realized long time back that problems in algebra, number theory and even geometry can be solved using very similar techniques. They were interested in finding out the common element among these proofs and were interested in searching for more domains where such techniques are applicable. It turns out that there is a single mathematical theory which can help us understand these questions in a single framework and give us answers to these seemingly non-related topics.

The mathematical framework which ties these questions together is called *abstract algebra*. Not surprisingly, given the name, the course is going to be about *abstract algebra*.

Exercise 1.1. What does *abstract* mean?

Note 1.2. The exercises given in the course notes are practice problems with the exception of this particular introduction. The exercises given in this particular document are to motivate the study of abstract algebra. You should try to think about them but remember that there are no clear answers.

We will precisely study the mathematical structures which can represent numbers, matrices, permutations, geometric objects under different parameters. The first step would be to define these mathematical (algebraic) structures like groups, rings and fields. The next step is to find properties of these algebraic

structures. Finally we will also see how these properties give so many beautiful results in different areas of mathematics.

Lets start with a more basic question,

Exercise 1.3. What does *algebra* mean?

1.1.1 Arithmetic and algebra

Most of the people when asked the above question, think about numbers, equations and operations between them. So lets make the previous question more precise. What is the difference between arithmetic and algebra? Arithmetic is the study of numbers and the operations (like addition, subtraction, multiplication) between them. Algebra, intuitively, talks about equations, variables, symbols and relations between them.

The primary difference is the use of variables, which can stand for an unknown or a group of numbers. These variables are somewhat abstract but really help us in manipulating equations and solving them. It would be too cumbersome to write things in words instead of using equations and variables.

Exercise 1.4. Give an example where using a variable helps you to write a statement concisely.

Now we know what algebra is, lets talk about *abstract* part of it.

1.1.2 Abstraction

All of us like numbers (or at least understand the importance of it). One of the reason is that numbers are very well-behaved. In other words, there are so many nice properties that it is easy to manipulate and work with numbers. Lets look at one of the most fundamental properties,

Theorem 1.5. *Fundamental theorem of arithmetic: Every integer greater than* 1 *can be uniquely expressed as the product of primes up to different orderings.*

Since this property is so useful, we should ask, are there other objects which satisfy similar theorems.

Exercise 1.6. Do we have unique factorization theorem for matrices or permutations.

There is a very important methodology to generalize given proofs. You look at the proof and figure out the crucial step and properties which make the proof work. So one way to approach this question would be, carefully look at the proof of the theorem and figure out the properties of integers we have used at different step. Then check if another mathematical object satisfies the same properties.

In other words, *any* mathematical object which satisfies these properties will also have a unique factorization theorem. The abstract object which has all these properties can be given an appropriate name. This is similar to variables. As variables can take different values, this abstract object can be assigned different mathematical objects.

We will turn this method upside down. We will consider some basic properties and give a name to the abstract structure which satisfies these "basic properties".

Exercise 1.7. Who decides these basic properties?

Using these "basic properties" we will come up with multiple theorems like the unique factorization theorem above. By the above discussion any mathematical object (from arithmetic, algebra, geometry or anywhere else) which has these "basic properties" will satisfy all the theorems too. Hence in one shot we will get theorems in diverse areas.

You are already familiar with one such abstract structure, *set*. A collection of objects is called set and it needs no other property to be satisfied.

Exercise 1.8. What kind of theorems can you prove for sets?

In the course we will look at the collection of objects (sets) with certain composition properties. These will give rise to groups, rings etc.. The first such abstraction we will study is group.

Exercise 1.9. Should we choose as many basic properties as possible or as less basic properties as possible?

2

Groups

These notes are about the first abstract mathematical structure we are going to study, *groups*. You are already familiar with *set*, which is just a collection of objects. Most of the sets we encounter in mathematics are useful because of the operations we can perform on them. We can do addition, multiplication, AND, OR, take power etc..

Sets, by definition, need not have such operations. For example, $S = \{Apple, Oranges, CS203, Monitor\}$ is a set. But, if we look at more interesting sets like integers, matrices, permutations etc., we generally have operations which can be done on them. For example, you can add matrices, multiply permutations, add and multiply integers and so on.

Our next task is to define an abstract object (say a special set) with operation to compose elements inside the object. But first lets ask a basic question. What are the nice properties of addition of two natural numbers? What about integers?

To begin with, it is great that we can add two numbers, that is, the addition of any two numbers is a number. Another property not present in natural numbers is that we can always solve $a + x = b$ (a, b are given, x is unknown). Notice that we have to assume the existence of *Zero*.

Exercise 2.1. Can you think about other properties? Do they follow from the properties mentioned above?

2.1 Groups

A group G is a set with binary operation $*$, s.t.,

1. Closure: For any two elements $a, b \in G$; their composition under the binary operation $a * b \in G$.
2. Associativity: For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$. This property basically means that any bracketing of $a_1 * a_2 * \cdots * a_k$ is same (exercise).
3. Identity: There is an element *identity* (e) in G, s.t., $a * e = e * a = a$ for all $a \in G$.
4. Inverse: For all $a \in G$, there exist $a^{-1} \in G$, s.t., $a * a^{-1} = a^{-1} * a = e$.

Note 2.2. Some texts define binary operation as something which has *closure* property. In that case, the first property is redundant. For the sake of brevity, it is sometimes easier to write xy instead of $x * y$.

Sometime we denote a group by its set and the operation, e.g., $(\mathbb{Z}, +)$ is the group of integers under addition.

Exercise 2.3. Show that integers form a group under addition (In other words, Integers have a group structure with respect to addition). Do they form a group under multiplication?

You can think of groups as being inspired by integers. In other words, we wanted to abstract out some of the fundamental properties of integers. We will later see that all groups share some properties with integers, but more interestingly, there are a lot of other groups which do not look like integers. That means there are

some properties of integers which are not captured by the definition of groups. So what properties of integers do you think is not captured by groups?

To start with, we haven't specified *commutativity* as one of the basic properties. The properties are chosen so that we have many examples of groups and simultaneously we can prove a lot of theorems (properties) of this group structure. Later we will see that some important groups do not have commutativity property.

Definition 2.4. *A group is called* commutative *or* abelian *if,* $\forall a, b \in G; a * b = b * a$.

2.1.1 Examples of groups

Exercise 2.5. Can you think of any other group except integers under addition? Is it commutative?

The whole exercise of abstraction will be a waste if integers (addition) is the only set which follow group property. Indeed, there are many examples of groups around you, or at least in the mathematics books around you.

- Integers, Rationals, Reals, Complex numbers under addition. Clearly for all these 0 is the identity element. The inverse of an element is the negative of that element.
- Rationals, Reals, Complex numbers (without zero) under multiplication. Identity for these groups is the element 1. Why did we exclude integers?
- Positive rationals, positive reals under multiplication.
- The group $\mathbb{Z}_n$, set of all remainders modulo n under addition modulo n. Will it be a group under multiplication? How can you make it a group under multiplication?

Till now all the examples taken are from numbers. They are all subsets of complex numbers. Lets look at a few diverse ones.

- The symmetries of a regular polygon under composition. In other words, the operations which keep the polygon fixed. The symmetries are either obtained through rotation or reflection or combination of both. This group is called *Dihedral group*.
- The set of all permutations of $\{1, 2, \cdots, n\}$ under composition. What is the inverse element?
- The set of all $n \times n$ matrices under addition. The identity in this case is the all 0 matrix,

$$\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

- The set of all $n \times n$ invertible matrices of real numbers. What is the identity element?

We have seen so many examples of groups. Are they all *similar* (we will define the word *similar* later). Can we represent a group in a succinct way. One of the trivial representation is the *multiplication table* of the group. It is a matrix with rows and columns both indexed by group elements. The $(i, j)^{th}$ entry denotes the sum of i^{th} and j^{th} group element. For example, lets look at the multiplication table of $\mathbb{Z}_5^+$ under multiplication. Here $\mathbb{Z}_5^+$ denotes all the remainders modulo 5 Co-prime to 5 (gcd with 5 is 1).

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Exercise 2.6. Notice that every element occurs exactly once in every row and every column. Do you think this property is true for any group or just $\mathbb{Z}_5$?

Multiplication table gives us all the information about the group but is a pretty long description. Specifically it is quadratic in the size of the group. It turns out that groups have lot of properties which can help us in giving a more succinct representation. We already showed one property, that the identity is unique. What other theorems can be shown for groups?

2.2 Properties of groups

To start with, we need to define few quantities. Suppose we are given an element $x \neq e$ of group G. What other elements can be constructed with x. The composition with identity will not give anything new, so lets compose it with itself. Since G is a group, $x^2 := x * x, x^3 := x^2 * x$ (notice the new notation) and so on will be elements of group G. In this way we can create new elements in G except if these elements start repeating.

Suppose G is finite, then sooner or later there will exist i and j, s.t., $x^i = x^j$.

Exercise 2.7. Show that the first element which will repeat is e.

The least positive j for which $x^j = e$ is called the *order* of x and is denoted by $|x|$. Clearly the only element with order 1 is e and everything else will have a bigger order.

We will now go on to prove more properties of groups, but before that there is a warning. Groups are inspired by numbers and the notations are very similar. It is not surprising that sometimes you can get carried away and use properties of integers which are not really true for groups (e.g., commutativity).

For all the proofs for the theorems given below, notice that we will use the already known properties like closure, associativity, inverse, existence of identity. Then using those theorems we can prove other results. Now check your proofs for the exercises given in this section above.

This distinction can be made more clear by an analogy which we will use later too. Working with groups is like playing *football*. In general, for any activity you use your hands, feet or any other tool. But in case of football there is a restriction that you only use your feet. Using your feet you develop other skills which can be used to score a goal.

Our goal would be to prove theorems. Our feet will be the defining properties of groups (closure, associativity, inverse, identity). And the intermediate theorems would be like dribbling or kicking. You should not foul (use properties of integers) to prove a theorem (score a goal). So lets play football. We will use G to denote a group.

- The inverse of an element is unique.
  Proof: Suppose a has two inverses b and c. Then $c = (ba)c = b(ac) = b$. What properties of groups did we use in this proof.
- Cancellation laws: Given $a, b, x \in G$, we know $ax = bx \Rightarrow a = b$, and also $xa = xb \Rightarrow a = b$. These are called respectively the right and the left cancellation law.

  Exercise 2.8. Prove the assertion. What does it say about the rows (or columns) of multiplication table?

- $x \in G$ and x^{-1} have the same order.
  Proof: We will show that order of x^{-1} is at most the order of x, by symmetry this will prove the assertion. Suppose $x^n = e$. Multiply this equality by x^{-n} and we get $x^{-n} = e$ and hence the order of x^{-1} is less than n.

  Exercise 2.9. We did not define x^{-n}. What do you think it should be?

For a finite group we have shown that its order is less than the cardinality (also called the order) of the group. Actually order of an element can be restricted to just the divisors of the order of the group. Look carefully at the following theorem and proof.

Theorem 2.10. *Suppose G is a finite group with n elements (n is the order of the group). If d is the order of an element $x \in G$ then n is a multiple of d ($d \mid n$).*

Proof. We will prove the theorem in two steps. First, we will show that $x^n = e \ \ \forall x \in G$. Second, if there is any m, s.t., $x^m = e$ then d divides m. From these two steps the conclusion can be easily inferred.

From the cancellation laws, it is clear that $S_x = \{xg : g \in G\} = G$ as a set. All elements of S_x are distinct, in G and hence they are just a permutation of elements of G. Taking the product over all elements of S_x,

$$\Pi_{s \in S_x} s = \Pi_{g \in G} xg = x^n \Pi_{g \in G} g = x^n \Pi_{s \in S_x} s.$$

Using the first and the last step,

$$e = x^n.$$

So for every element $x \in G$, we know $x^n = e$.

For the second part, suppose $m = kd + r$ by division. Here k is the quotient and $r < d$ is the remainder. Then looking at x^m,

$$e = x^m = x^{kd+r} = x^r.$$

So there exist $r < n$, s.t. $x^r = e$. By the definition of order, $r = 0$. Hence d divides m.

Actually the proof given above is not correct.

Exercise 2.11. Where is the mistake in the proof? Hint: It is in the first part.

□

If you look at the proof of fact that $x^n = e$, then it was proved using commutativity. So we have only proved that for a *commutative* or *abelian* group the thm. 2.10 is true. It turns out that it is true for non-commutative groups too. We will prove the full generalization later with a different technique.

2.3 Isomorphism and homomorphism of a group

As discusses above we want to find out what kind of groups are there. Are they all *similar*. Let us formalize the notion of similarity now. Clearly if two sets are equal if and only if there is a bijection between them. But the bijection need not respect the composition. That means the composition properties of two groups might be completely different even if they have a bijection between them.

Exercise 2.12. Would you say that groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_8^+, \times)$ similar (both have four elements). The second group is the set of all remainders modulo 8 which are Co-prime to 8.

Hint: Look at the orders of different elements in these groups.

Hence for group similarity, we need to take care of composition too. Two groups are considered same if they are *isomorphic* to each other. In other words there exist an *isomorphism* between the two. To define, a group G_1 is isomorphic to group G_2, if there exist a bijection $\phi : G_1 \to G_2$, s.t.,

$$\forall g, h \in G_1 : \quad \phi(g)\phi(h) = \phi(gh).$$

The second property takes care of the composition. A related notion is called *homomorphism* where we drop the bijection criteria. So G_1 is homomorphic to G_2 if there exist a *map* $\phi : G_1 \to G_2$, s.t.,

$$\forall g, h \in G_1 : \quad \phi(g)\phi(h) = \phi(gh).$$

Exercise 2.13. Give a homomorphism which is not an isomorphism from a group G to itself.

2.4 Assignment

Exercise 2.14. For any $a_1, a_2, \cdots, a_k \in G$, show that expression $a_1 * a_2 * \cdots * a_k$ is independent of bracketing.

Hint: Show it using induction that all expression are same as $a_1 * (a_2 * (\cdots * a_k) \cdots)$.

Exercise 2.15. Prove that the identity is unique for a group.

Exercise 2.16. Which Groups are commutative from the list of groups given in the section 2.1.1?

Exercise 2.17. Prove that $G = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a group under addition.

Exercise 2.18. Which of them are groups under addition?

- The set of all rational numbers with absolute value < 1.
- The set of all rational number with absolute value ≥ 1.
- The set of all rational numbers with denominator either 1 or 2 in the reduced form.

Exercise 2.19. Find the order of following,

- 3 in $\mathbb{Z}_5, +$.
- 5 in $\mathbb{Z}_7, \times$.
- Transpositions in permutations. What about product of disjoint transpositions?

Exercise 2.20. Give an example of a finite group where order of an element is different from order of the group.

Exercise 2.21. If all elements have order 2 for a group G, prove that it is abelian.

Exercise 2.22. Show that if G_1 is isomorphic to G_2 then G_2 is isomorphic to G_1.

Exercise 2.23. Show an isomorphism from real numbers with addition to positive real numbers with multiplication.

3

Subgroups

We are interested in studying the properties and structure of the group. By properties, we mean the theorems which can be proven about groups in general. Then any mathematical construct having the group structure (satisfy closure, associativity etc.) will satisfy those theorems.

Another important task is to understand the structure of group itself. It is deeply related to the properties of group. It ultimately helps us in figuring out which groups are similar (with respect to isomorphism) and can we list out all possible kind of groups (not isomorphic to each other).

One of the natural question is that if groups can exist inside a group.

Exercise 3.1. Can we have a subset of group which itself is a group under the group operation? Try to construct such a set in $\mathbb{Z}$.

3.1 Definition

As the intuition would suggest,

Definition 3.2. *A subset H of a group G is called a subgroup if it is not empty, closed under group operation and has inverses. The notation $H \leq G$ denotes that H is a subgroup of G.*

Note 3.3. The subgroup has the same operation as the original group itself

Exercise 3.4. Why did we not consider associativity, existence of inverse?

Every group G has two trivial subgroups, e and the group G itself. Lets look at few examples of non-trivial subgroups. Try to prove that each of them is a subgroup.

- $n\mathbb{Z}$, the set of all multiples of n is a subgroup of Integers.
- Under addition, integers ($\mathbb{Z}$) are a subgroup of Rationals ($\mathbb{Q}$) which are a subgroup of Reals ($\mathbb{R}$). Reals are a subgroup of Complex numbers, $\mathbb{C}$.
- $\mathbb{Z}^+$, the set of all positive integers is not a subgroup of $\mathbb{Z}$. Why?
- The set $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a subgroup of $\mathbb{R}$ under addition.
- Center of a group: The *center* of a group G is the set of elements which commute with every element of G.

  $$C(G) = \{h \in G : \ hg = gh \ \ \forall g \in G\}.$$

  We will show that center is the subgroup. Associativity follows from G and existence of identity is clear. Suppose $h, k \in C(G)$, then for any $g \in G$,

  $$g(hk) = hgk = (hk)g.$$

  Hence $C(G)$ is closed. For the inverse, note that $gh = hg$ is equivalent to $h^{-1}gh = g$ and $g = hgh^{-1}$. Hence existence of inverse follows (Why?).

3.1.1 Cyclic groups

We noticed that $\{e\}$ is a subgroup of every group. Lets try to construct more subgroups. Suppose x is some element which is not the identity of the group G. If k is the order of x then $S_x = \{e, x, x^2, \cdots, x^{k-1}\}$ is a set with all distinct entries. It is clear from previous discussion of groups that S_x is a subgroup.

Exercise 3.5. Prove that S_x is a subgroup.

While proving the previous exercise, we need to use the fact that k is finite. What happens when k is infinite? Can we construct a group then? The answer is yes, if we include the inverses too. All these kind of groups, generated from a single element, are called *cyclic groups.*

Definition 3.6. *A group is called* cyclic *if it can be* generated *by a single element. In other words, there exist an element $x \in G$, s.t., all elements of G come from the set,*

$$< x >= \{\cdots, x^{-2}, x^{-1}, e, x, x^2, \cdots\}$$

There are many things to note here:

- For an infinite group, we need to consider inverses explicitly. For a finite group, inverses occur in the positive powers.
- The group *generated* by the set S is the group containing all possible elements obtained from S through composition (assuming associativity, inverses etc.).
- The notation for the group generated by S is $< S >$.

The structure of cyclic groups seem very simple. You take an element and keep composing. What different kind of cyclic groups can be there? Look at different examples of cyclic groups of order 4 in figure 3.1.1. The next theorem shows that all these are isomorphic.

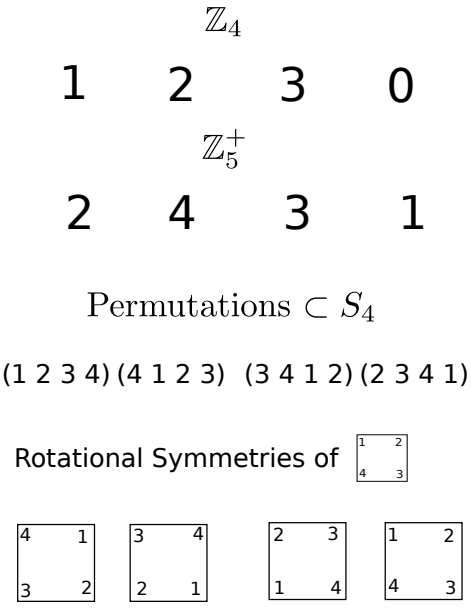

Fig. 3.1. Different cyclic groups

Theorem 3.7. *Every finite cyclic group G of order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Suppose x is a generator for G. It exists by the definition of G. Then since the order is finite, group G is,

$$G = \{e, x, x^2, \cdots, x^{n-1}\}$$

Lets look at the obvious bijection ϕ from $\mathbb{Z}_n$ to G. The element k is mapped to x^k. It is a bijection because, the inverse maps x^k to k. For the above bijection,

$$\phi(j+k) = x^{j+k \mod n} = x^j * x^k = \phi(j) * \phi(k).$$

Where first inequality follows from the definition of $\mathbb{Z}_n$ and second from the fact that $x^n = 1$. This shows that ϕ is an isomorphism. Hence Proved. □

Using the previous theorem and exercise (assignment), we have given complete characterization of cyclic groups. This loosely means that we can get all the properties of any cyclic group of order n from $\mathbb{Z}_n$ and an infinite cyclic group with integers.

This is called a *classification* of cyclic groups. We would ideally like to give classification of groups and finding out more properties of groups. These two questions are not independent. We will explore both simultaneously and progress in one question helps in finding the answer for other.

Exercise 3.8. What are the subgroups of a cyclic group?

3.2 Cosets

The next step in understanding the structure of a group is to partition it using a subgroup. Suppose we are given a group G and its subgroup H. We will show that G can be partitioned into disjoint sets of equal size ($|H|$). This will imply that $|G|$ is always divisible by $|H|$. Lets define these parts first and then we can prove the fact given above.

Definition 3.9. *Cosets: The* left coset *(gH) of H with respect to an element g in G is the set of all elements which can be obtained by multiplying g with an element of H,*

$$gH = \{gh : \quad h \in H\}.$$

This is called the left coset because g is multiplied on the left. We can similarly define the right cosets Hg.

Exercise 3.10. How are left and right coset related for commutative groups?

Let us show some properties of these cosets. Remember not to use any illegal property while proving these. Without loss of generality we will assume that cosets are left. Same properties hold true for right ones too.

- Every element of G is in at least one coset. H is one of the cosets too.

  Proof. Exercise. □

- The cardinality of all cosets is equal and hence their cardinality is $|H|$.

  Proof. Consider a coset gH and a subgroup $H = \{h_1, h_2, \cdots, h_k\}$. The elements of the left coset gH are $\{gh_1, gh_2, \cdots, gh_k\}$. It is easy to show that any two elements in this set are distinct (why?). Hence all cosets have cardinality $k = |H|$. □

- For any two elements g_1, g_2 of G either g_1H, g_2H are completely distinct (disjoint) or completely same ($g_1H = g_2H$).

Proof. Suppose there is one element common in g_1H and g_2H (otherwise they are completely distinct). Say it is $g_1h_1 = g_2h_2$, then,

$$g_1 = g_2h_2h_1^{-1} \rightarrow \exists\ h \in H :\ g_1 = g_2h.$$

Now you can prove a simple exercise.

Exercise 3.11. If $\exists\ h \in H :\ g_1 = g_2h$ then show that $g_1H \subseteq g_2H$.

But if $g_1 = g_2h$ then $g_2 = g_1h^{-1}$. This will show from the previous exercise that $g_2H \subseteq g_1H$. Hence both the sets g_1H and g_2H are the same. □

Using the properties we have shown that the two columns of the following table are completely the same or completely distinct.

G/H	e	g_2	$\cdots$	g_n
e	e	g_2	$\cdots$	g_n
h_2	h_2	g_2h_2	$\cdots$	g_nh_2
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
h_k	h_k	g_2h_k	$\cdots$	g_nh_k

This conclusion is beautifully summarized in Lagrange's theorem.

3.2.1 Lagrange's theorem

Using the previous list of properties it is clear that if we look at the distinct cosets of H then they partition the group G into disjoint parts of equal size.

Exercise 3.12. What is the size of these parts?

Theorem 3.13. *Lagrange: Given a group G and a subgroup H of this group, the order of H divided the order of G.*

Proof. The proof is left as an exercise. You should try to do it without looking at the hint given in the next line.

Hint: From the previous discussion, the $\frac{|G|}{|H|}$ is just the number of distinct cosets of H. □

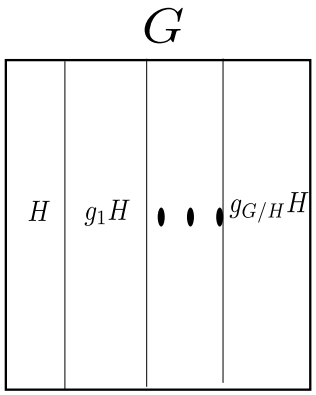

Fig. 3.2. Coset decomposition

Note 3.14. If the set of left and right cosets coincide the subgroup is called *normal*. In this case, the set of cosets actually forms a group, called the *quotient group* $\frac{G}{H}$ (What is the composition rule?).

This is a great discovery. The statement of Lagrange's theorem does not do justice to the implications. We started with an abstract structure with some basic properties like associativity, inverses etc. (group). The proof of Lagrange's theorem implies that if we can find a subgroup of the group then the whole group can be seen as a disjoint partition with all parts related to the subgroup. Notice that it is easy to construct a cyclic subgroup of a group.

Exercise 3.15. Prove that the order of an element always divides the order of a group. We had proved this for commutative groups in an earlier lecture.

Exercise 3.16. What does Lagrange's theorem say about groups with prime order?

Lets look at one application of Lagrange's theorem in the case of $\mathbb{Z}_m^\times$. We know that this group contains all the remainders mod m which are coprime (gcd is 1) to m. If m is a prime p then $\mathbb{Z}_p^\times$ contains $p-1$ elements. This proves the well known *Fermat's little theorem.*

Exercise 3.17. Fermat's little theorem: For a prime p and any number a,

$$a^{p-1} = 1 \mod p.$$

Prove this theorem.

3.3 Dihedral group

Till now most of the exercises we have done are for $\mathbb{Z}$ and $\mathbb{Z}_n$. These groups are commutative. This section will introduce you to a non-commutative subgroup.

Definition 3.18. *A Dihedral group D_{2n} is the group of symmetries of a regular n-gon.*

A regular n-gon can be rotated or reflected to get back the n-gon. The group D_{2n} is the group generated by reflection s and rotation r by the angle $\frac{2\pi}{n}$. Refer to figure 3.3 for all the symmetries of a pentagon.

For an $n-gon$ there are n rotations possible. The set of rotations form a cyclic group of order n.

Exercise 3.19. What is the inverse of rotation r. Convince yourself that set of rotations form a cyclic group.

On the other hand reflection is the inverse of itself. Hence it is an element of order 2. From the figure you can guess that there will be $2n$ symmetries of the form $s^i r^j$, where i ranges in $\{0,1\}$ and j is an element from $\{0,1,\cdots,n-1\}$. Using this notation, rs means we apply s first and then r.

Exercise 3.20. Convince yourself that $rs \neq sr$.

Notice that we have given a description of $2n$ elements of the dihedral group D_{2n}. How can we be sure that there are no more elements generated by r and s. What about $rsrs$?

Exercise 3.21. Show that $rs = sr^{-1}$.

This relation tell us how to interchange r and s in any expression involving both. This way we can convert any element of the group generated by r and s to be of the form $s^i r^j$ with i and j ranging appropriately.

The above discussion shows the important properties (defining properties) of dihedral group.

- An element of order 2, s.
- An element of order n, r.
- The commutation relation $rs = sr^{-1}$.
- $s \neq r^i$ for any i.

Any group which is generated by two elements with the above mentioned properties will be isomorphic to D_{2n}.

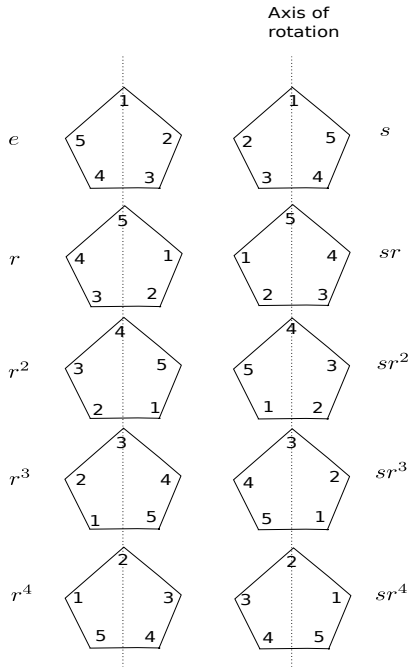

Fig. 3.3. Symmetries of a pentagon

3.4 Assignment

Exercise 3.22. List all possible subgroups of $\mathbb{Z}_6$ under addition.

Exercise 3.23. The *kernel* of a homomorphism $\phi : G \to L$ is the subset of G which maps to identity of L. Hence,

$$Ker(\phi) = \{g \in G : \ \phi(g) = e_L\}.$$

Similarly, the *image* of ϕ are the elements of L which have some element mapped to them through ϕ.

$$Img(G) = \{h \in L : \ \exists g \in G \text{ for which } \phi(g) = h.\}$$

show that $Img(G)$ and $Ker(G)$ are subgroups.

Exercise 3.24. Show that a subset H is a subgroup of G if it is non-empty and $\forall x, y \in H : \ xy^{-1} \in H$.

Note 3.25. Because H is a subset, the set of properties we need to check are much less.

Exercise 3.26. Show that $\mathbb{Z}_n$ is cyclic under addition. Give some examples of cyclic subgroups and some examples of non-cyclic subgroups in $\mathbb{Z}_n^+$ under multiplication.

Exercise 3.27. Show that all cyclic groups are commutative (abelian).

Exercise 3.28. Show that every cyclic group with infinite order (having infinite elements) is isomorphic to $\mathbb{Z}$ under addition.

Hint: Look for the obvious bijection between the group and $\mathbb{Z}$. Show that it is an isomorphism.

Exercise 3.29. Find the order of every element of group $\mathbb{Z}_p$ where p is a prime.

Exercise 3.30. Find the left cosets of $3\mathbb{Z}$ in group $\mathbb{Z}$.

Exercise 3.31. If order of a group G is prime p then show that it is isomorphic to $\mathbb{Z}_p$.

Exercise 3.32. Euler's theorem: For a number m, say $\phi(m)$ is the number of positive elements coprime to m and less than m. For any a which is co-prime to m,

$$a^{\phi(m)} = 1 \mod m.$$

Prove this theorem.

Exercise 3.33. Show that there always exist a cyclic subgroup of any finite group G.

Exercise 3.34. Show that the subgroup of a cyclic group is cyclic.

4

Orbits

In the beginning of the course we asked a question. How many different necklaces can we form using 2 black beads and 10 white beads? In the question, the numbers 2 and 10 are arbitrarily chosen. To answer this question in a meaningful way, we need to construct a strategy or theorem which will answer the above question for any such numbers. But to understand the question better, lets ask a simpler question.

Exercise 4.1. How many different necklaces can be formed using 2 white and 2 black beads?

Lets look at the question in detail. The first guess for the question would be $4! = 24$, the number of ways we can permute the four beads. But all these permutations need not be different. What do we mean by *different* necklaces? It might happen that two different permutations (σ_1 and σ_2) might be the same in the sense that σ_1 can be obtained from σ_2 using rotation. Look at figure 4 for one such example.

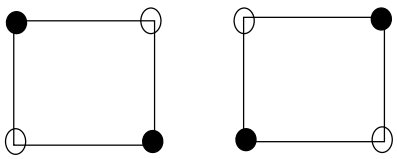

Fig. 4.1. Two permutations giving the same necklace

Using some brute force now, we can come up with all possible different necklaces for 2 white and 2 black beads (figure 4).

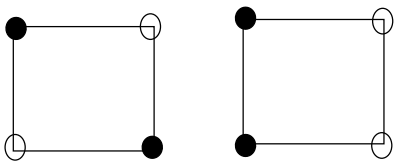

Fig. 4.2. Possible different necklaces with 2 white and 2 black beads

You can convince yourself that the question is much harder if we take bigger numbers. What should we do? When are two necklaces equivalent?

Two necklaces are equivalent if we can obtain one by applying a symmetry to other necklace (like rotation or reflection). We know from discussions in previous classes that the symmetries form the dihedral group, D_{2n}. The strategy would be to develop a general framework for groups to answer question about distinct necklaces.

4.1 Group action

The first thing to notice in the necklace problem is that there are two different objects of interest. One is the set of necklaces (set of all permutations of the necklaces) and other is the set of symmetries. A symmetry can be applied to a necklace to obtain another necklace. Lets make this action abstract.

Abstractly, given a group G and a set A, every element g of G *acts* on set A. That means for every element g there is a function from A to A which is called its action on G. For the sake of brevity, we will denote the function corresponding to the element $g \in G$ with g itself. Hence the value of $a \in A$ after action of g will be called $g(a)$.

Exercise 4.2. What is the group and what is the set for the necklace problem?

Note 4.3. It is NOT the set of distinct necklaces.

Lets look at the formal definition.

Definition 4.4. *Given a group G and a set A, a group action from G to A assigns a function $g : A \to A$ for every element g of group G. A valid group action satisfies the following properties.*

- *Identity takes any element $a \in A$ to a itself, i.e., $e(a) = a$ for every $a \in A$.*
- *For any two group elements $g_1, g_2 \in G$, their functions are consistent with the group composition,*

$$g_1(g_2(a)) = (g_1 g_2)(a).$$

Using this definition and group structure of G, it can be shown that action of g is a permutation on the elements of A.

This gives us another representation of group elements. For any group action on A of size m, we have a permutation representation for any element $g \in G$ in terms of a permutation on m elements. In the following sections we will keep this representation in mind.

Note 4.5. Actually a slightly stronger theorem holds. It is called *Cayley's theorem* and is given below. We will not show the proof of this theorem.

Theorem 4.6. *Cayley's theorem: Every group of order n is isomorphic to some subgroup of S_n.*

4.2 Orbits

Suppose we are given action of group G on a set A. Lets define a relation between the elements of A. If $\exists\ g :\ g(x) = y$ then we will say that x, y are related ($x \sim y$). We can easily prove that this relation is equivalence relation.

- Reflexive: Why?
- Symmetric: Suppose $x \sim y$ because $g(x) = y$. Then consider $x = ex = (g^{-1}g)(x) = g^{-1}y$, implying $y \sim x$.
- Transitive: Show it as an exercise.

Hence this equivalence relation will partition the set A into distinct equivalence classes. The equivalence class corresponding to $x \in A$ is the orbit ($G(x)$) of element x. In other words,

$$G(x) = \{g(x) :\ g \in G\}.$$

Now we will look at two counting questions,

1. What is the size of these orbits?
2. How many distinct orbits are there?

Why are we interested in these questions. Let us look at this concept from the example of necklaces. If a necklace x can be obtained from another necklace y using a symmetry then they are related (in the necklace case indistinguishable).

Exercise 4.7. Convince yourself that the number of distinct necklaces is the same as the number of distinct orbits (equivalence classes) under the dihedral group D_{2n}.

We will answer both the counting questions under the general group-theoretic framework. As a special case, this will solve the necklace problem.

4.2.1 stabilizers

Remember that the orbit of $x \in A$ under the action of G can be defined as,

$$G(x) = \{g(x) : \ g \in G\}.$$

If every $g \in G$ took x to a different element, the size of the orbit would be $|G|$. But this is too much to expect. If we consider any example, there will be lots of $g \in G$ which will take x to a single element y. Lets define this set as G(x,y),

$$G(x, y) = \{g \in G : \ g(x) = y\}.$$

Exercise 4.8. Does the set $G(x, y)$ form a subgroup of G? Under what condition will it form a subgroup?

The answer to the previous exercise is when $x = y$. The set $G_x := G(x, x)$ is called the stabilizer of x,

$$G_x = \{g \in G : \ g(x) = x\}.$$

Exercise 4.9. If you were not able to solve the previous exercise, prove that G_x is a subgroup of G.

Once we have the subgroup G_x, the natural question to ask is, what are the cosets? This is where we get lucky. Suppose y is an element of the orbit $G(x)$. So there exist an $h \in G$, s.t., $h(x) = y$. Then $G(x, y)$ is precisely the coset hG_x.

Lemma 4.10. *Given a $y \in A$, s.t., $h(x) = y$. The coset hG_x is same as the set $G(x, y)$.*

Proof. $\Rightarrow$: An element of hG_x is of the form $hg, \ g \in G_x$. Then $hg(x) = h(x) = y$. So $hG_x \subseteq G(x, y)$.
$\Leftarrow$: Suppose $g \in G(x, y)$, i.e., $g(x) = y$. Then show that,

Exercise 4.11. $h^{-1}g \in G_x$

But $h^{-1}g \in G_x$ implies $g \in hG_x$.

Exercise 4.12. Show the above implication. Be careful, It is not just the same as multiplying by h on both sides.

From the previous exercise $G(x, y) \subseteq G_x$. □

Hence, for every element y in the orbit $G(x)$, there is a coset. It is an easy exercise to convince yourself that every coset will correspond to a single element in the orbit $G(x)$. So the number of elements in the orbit is equal to the number of cosets. But we know that the number of cosets can be calculated from Lagrange's theorem. Hence,

$$|G| = |G_x||G(x)|.$$

Note 4.13. G_x is a subset of G, but $G(x) \subseteq A$. The equation works because we show a one to one relation between $G(x)$ (orbit) and the cosets.

4.2.2 Burnside's lemma

We now know the size of the orbit. Given an element x with stabilizer G_x, the number of elements in its orbit is $\frac{|G|}{|G_x|}$. Can this help us in counting the number of distinct orbits.

Lets give every element on A a weight of $\frac{1}{|G(x)|}$. The number of distinct orbits is now the sum of weights of all elements of A.

$$\text{Number of distinct orbits } = \sum_{x \in A} \frac{1}{|G(x)|} = \frac{1}{|G|} \sum_{x \in A} |G_x|.$$

Lets concentrate on the summation. The total summation is equal to the number of pairs $(g \in G, x \in A)$, s.t., $g(x) = x$. Suppose we make a matrix with rows indexed by elements of G and columns indexed by elements of A. The entry (g, x) is one if $g(x) = x$ and 0 otherwise.

	x_1	x_2	$\cdots$	$x_{\lvert A\rvert}$
g_1	0	1	$\cdots$	1
g_2	0	0	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$g_{\lvert G\rvert}$	1	0	$\cdots$	0

Then $\sum_x |G(x)|$ is the number of 1's in the matrix above. Each term in the summation, $|G_x|$ is the number of 1's in the column corresponding to x. We can count the number of 1's in the matrix by taking the sum row-wise too. Suppose, $S(g)$ is set of elements of A fixed by g.

$$S(g) = \{x : \ g(x) = x, \ x \in A\}.$$

Using $S(g)$ we get the orbit-counting (Burnside's) lemma.

Lemma 4.14. *Burnside's lemma (Orbit-counting): Given a group action of G over A. The number of distinct orbits can be written as,*

$$\textit{Number of distinct orbits } = \frac{1}{|G|} \sum_{g \in G} |S(g)|.$$

Note 4.15. The summation is now over G instead of A.

One natural question you might ask is, How did this benefit us? Previously we were summing over all possible $x \in A$ and now we are summing up over all $g \in G$. The reason is, in general, the size G will be much smaller than size of A.

Lets look at an example where Orbit-counting lemma will help us in answering the question about necklaces. Try to solve this exercise yourself first and later you can look at the solution given below.

Exercise 4.16. How many necklaces can be formed with 2 black and 6 white beads?

Arrange the beads on the vertices of a regular 8-gon. Since the necklaces are obtained by fixing the position of 2 black beads, there are 28 elements in A. The symmetry group is D_{16} with 16 elements.

For different elements of G we can calculate the number of elements fixed by it.

- Identity e: Fixes 28 elements.
- Out of 7 other rotations, only one of them fixes 4 elements. What is the angle of that rotation? Rest do not fix anything.
- All reflections fix exactly 4 elements. It is easy to see by looking at the cycle structure of the permutation. All beads of the same color should fall in the same cycle.

So by Orbit-counting lemma,

$$\text{Number of distinct orbits } = \frac{1}{16}(28 + 4 + 8 \times 4) = 4.$$

Exercise 4.17. What are the four configurations? Can you characterize them?

For other examples of application of Burnside's lemma, please look at section 21.4 of Norman Biggs book. There is a nice example in Peter Cameron's notes on Group Theory too (section 1.3).

4.3 Group representations (advanced)

We looked at the permutation representation of every group. There is a matrix representation of every group too. The study of that representation is called the group representation theory. Group representation theory is one of the main tools to understand the structure of a group. We will only give a very basic idea of this field. Interested students can look at book *Algebra* by Artin.

Define GL_n to be the group of invertible matrices of size $n \times n$ with complex entries. We can also think of these matrices as linear operators over $\mathbb{C}^n$.

A linear representation (matrix representation) is a homomorphism from group G to the group GL_n (say $R : G \to GL_n$). That means, we map every element of group G to an invertible matrix, s.t., it obeys the group composition,

$$R(gh) = R(g)R(h).$$

If there is a subspace of $\mathbb{C}^n$ which is fixed by every group element, then the representation is reducible. In other words, for an irreducible representation, there is NO subspace which is fixed by every element of group G.

Exercise 4.18. What does it mean that the subspace is fixed?

It can be shown that every representation can be broken down into irreducible representations. Another quantity of interest is the *character*. The character of the representation is a function $\chi : G \to \mathbb{C}$ defined by $\chi(g) = trace(R(g))$.

The characters of irreducible representations are orthonormal to each other and satisfy various other nice properties. Many theorems in group theory are derived by studying the characters of the group. Again, interested students can find more information in the book *Algebra* by Artin.

4.4 Assignment

Exercise 4.19. Show that action of dihedral group on the set of necklaces is a group action.

Exercise 4.20. Show that G is isomorphic to a subgroup of $S_{|A|}$. Remember that S_n is the group of permutations of $[n]$.

Hint: First show that action of g on A is a permutation and then use the consistency of group action with the group composition.

Exercise 4.21. Suppose we want to find the number of necklaces with m black and n white beads. What is the size of G and what is the size of A in terms of m, n?

Exercise 4.22. Prove that the average number of elements fixed by an element of group G under group action is an integer.

Exercise 4.23. Prove that GL_n is a group. What composition rule did you use?

Exercise 4.24. Biggs: Let G be a group of permutations of set A. If u, v are two elements in the same orbit of G, show that $|G_u| = |G_v|$.

Exercise 4.25. Biggs: Let A denote the set of corners of the cube and let G denote the group of permutations of A which correspond to rotation of the cube. Show that,

- G has just one orbit.
- For any corner x, $|G_x| = 3$.
- $|G| = 24$

Exercise 4.26. Biggs: Suppose you manufacture an identity card by punching two holes in an 3×3 grid. How many distinct cards can you produce. Look at the figure given below.

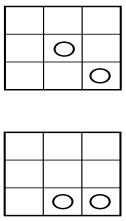

Fig. 4.3. Different identity cards with circles showing the holes.

Hint: The group to consider here is D_8.

5

Quotient group

We have seen that the cosets of a subgroup partition the entire group into disjoint parts. Every part has the same size and hence Lagrange's theorem follows. If you are not comfortable with cosets or Lagrange's theorem, please refer to earlier notes and refresh these concepts.

So we have information about the size of the cosets and the number of them. But we lack the understanding of their structure and relations between them. In this lecture, the concept of *normal subgroups* will be introduced and we will form a group of cosets themselves !!

5.1 Normal subgroup

Suppose we are given two elements g, n from a group G. The *conjugate* of n by g is the group element gng^{-1}.

Exercise 5.1. When is the conjugate of n equal to itself?

Clearly the conjugate of n by g is n itself iff n and g commute.

We can similarly define the conjugate of a set $N \subseteq G$ by g,

$$gNg^{-1} := \{gng^{-1} : \ n \in N\}.$$

Definition 5.2. *Normal subgroup: A subgroup N of G is* normal *if for every element g in G, the conjugate of N is N itself.*

$$gNg^{-1} = N \quad \forall g \in G.$$

We noticed that $gng^{-1} = n$ iff g, n commute with each other.

Exercise 5.3. When is $gNg^{-1} = N$?

In this case the left and right cosets are the same for any element g with respect to subgroup N. Hence, a subgroup is normal if its left and right cosets coincide.

Exercise 5.4. Show that following are equivalent. So you need to show that each of them applies any other.

1. N is a normal subgroup.
2. The set $S = \{g : gN = Ng\}$ is G itself.
3. For all elements $g \in G$, $gNg^{-1} \subseteq N$.

Hint: Instead of showing all $2 \times \binom{3}{2}$ implications, you can show 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1.

5.2 Quotient group

We have introduced the concept of normal subgroups without really emphasizing why it is defined. Lets move to our original question. What can be said about the set of cosets, do they form a group?

Suppose G is a group and H is a subgroup. Denote by S, the set of cosets of G with respect to H. For S to be a group it needs a law of composition. The most natural composition rule which comes to mind is,

$$(gH)(kH) = (gk)H.$$

Here gH and kH represent two different cosets. The problem with this definition is that it might not be *well-defined*. It might happen that $g' \in gH$ and $k' \in kH$ when multiplied give a totally different coset $(g'k')H$ then $(gk)H$.

Exercise 5.5. Show that this operation is well-defined for commutative (abelian) groups.

What about the general groups? Here comes the normal subgroup to the rescue.

Theorem 5.6. *Suppose G is a group and H is its subgroup, the operation,*

$$(gH)(kH) = (gk)H,$$

is well defined if and only if H is a normal subgroup.

Note 5.7. Every subgroup of a commutative group is normal.

Proof. $\Rightarrow$): We need to show that if the operation is well defined then $ghg^{-1} \in H$ for every $g \in G, h \in H$. Consider the multiplication of H with $g^{-1}H$. Since $e, h \in H$, we know $eH = hH$. Since the multiplication is well defined,

$$(eg^{-1})H = (eH)(g^{-1}H) = (hH)(g^{-1}H) = (hg^{-1})H \quad \Rightarrow \quad g^{-1}H = (hg^{-1})H.$$

Again using the fact that $e \in H$, $hg^{-1} \in g^{-1}H$. This implies $hg^{-1} = g^{-1}h' \quad \Rightarrow ghg^{-1} = h'$ for some $h' \in H$.

$\Leftarrow$): Suppose N is a normal subgroup. Given $g' = gn$ and $k' = kn'$, where $g, g', k, k' \in G$ and $n, n' \in N$, we need to show that $(gk)N = (g'k')N$.

$$(g'k')N = (gnkn')N.$$

Exercise 5.8. Show that there exist $m \in N$, s.t., $nk = km$. Hence complete the proof.

□

With this composition rule we can easily prove that the set of cosets form a group (exercise).

Definition 5.9. *Given a group G and a normal subgroup N, the group of cosets formed is known as the* quotient group *and is denoted by $\frac{G}{N}$.*

Using Lagrange's theorem,

Theorem 5.10. *Given a group G and a normal subgroup N,*

$$|G| = |N||\frac{G}{N}|$$

5.3 Relationship between quotient group and homomorphisms

Let us revisit the concept of homomorphisms between groups. The homomorphism between two groups G and H is a mapping $\phi : G \to H$ that preserves composition.

$$\phi(gg') = \phi(g)\phi(g')$$

For every homomorphism ϕ we can define two important sets.

- Image: The set of all elements h of H, s.t., there exists $g \in G$ for which $\phi(g) = h$.

$$Img(\phi) = \{h \in H : \quad \exists g \in G \quad \phi(g) = h\}$$

  Generally, you can restrict your attention to $Img(\phi)$ instead of the entire H.
- Kernel: The set of all elements of G which are mapped to identity in H.

$$Ker(\phi) = \{g \in G : \quad \phi(G) = e_H\}$$

  Notice how we have used the subscript to differentiate between the identity of G and H.

Note 5.11. $Img(\phi)$ is a subset of H and $Ker(\phi)$ is a subset of G.

Exercise 5.12. Prove that $Img(\phi)$ and $Ker(phi)$ form a group under composition with respect to H and G respectively.

Exercise 5.13. Show that $Ker(\phi)$ is a normal subgroup.

There is a beautiful relation between the quotient groups and homomorphisms. We know that $Ker(\phi)$ is the set of elements of G which map to identity. What do the cosets of $Ker(\phi)$ represent. Lets take two elements g, h of a coset $gKer(\phi)$. Hence $h = gk$ where $\phi(k) = e_H$. Then by the composition rule of homomorphism $\phi(g) = \phi(h)$.

Exercise 5.14. Prove that $\phi(g) = \phi(h)$ if and only if g and h belong to the same coset with respect to $Ker(\phi)$.

The set of elements of G which map to the same element in H are called the fibers of ϕ. The previous exercise tell us that fibers are essentially the cosets with respect to $Ker(\phi)$ (the quotient group).

The fibers are mapped to some element in $Img(\phi)$ by ϕ. Hence there is a one to one relationship between the quotient group $\frac{G}{Ker(\phi)}$ and $Img(\phi)$. Actually the relation is much stronger.

It is an easy exercise to show that the mapping between quotient group $\frac{G}{Ker(\phi)}$ and $Img(\phi)$ is an isomorphism.

Exercise 5.15. Prove that the above mapping is an isomorphism.

Again applying the Lagrange's theorem,

$$|G| = |Ker(\phi)||Img(\phi)|.$$

The figure 5.11 depict that every element of quotient group is mapped to one element of image of ϕ. Now we know that this mapping is *well-behaved* with respect to composition too.

$$\phi((gKer(\phi))(hKer(\phi))) = \phi(gKer(\phi))\phi(hKer(\phi))$$

There is an abuse of notation which highlights the main point also. The notation $\phi(gKer(\phi))$ represents the value of ϕ on any element of $gKer(\phi)$. We know that they all give the same value. The study of homomorphism is basically the study of quotient group. The study of quotient group can be done by choosing a representative for every coset and doing the computation over it (instead of the cosets).

We have shown that $Ker(\phi)$ is normal. It can also be shown that any normal subgroup N is a kernel of some homomorphism ϕ (exercise).

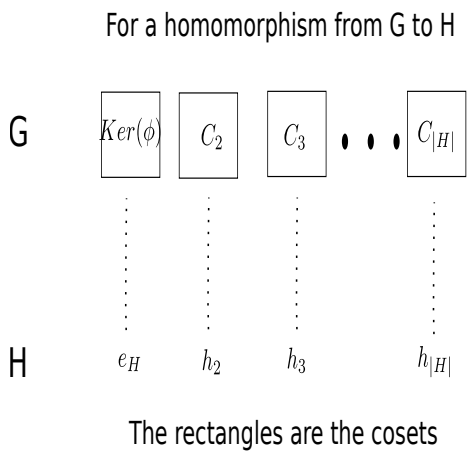

Fig. 5.1. Relationship between the quotient group and the image of homomorphism

5.4 Assignment

Exercise 5.16. Given a subgroup H of G, two elements $x, y \in G$ are related ($x \sim y$) if $x^{-1}y \in H$. Prove that this relation is an equivalence relation. What are the equivalence classes of this relation?

Exercise 5.17. Given a group G and a normal subgroup N. Say the set of cosets is called S and has composition operation $(gH)(kH) = (gk)H$. Show that,

- Identity exists in this set.
- Inverses exist in this set.
- Associativity is satisfied.

Since Closure is obvious we get that S is a group with respect to the above mentioned composition rule.

Exercise 5.18. Given a group G and a subgroup N as a set. Write a program to find if N is normal or not. Assume that you are given a function $mult(x, y)$, which can compute the binary operation of the group G between any two elements x, y of G.

Exercise 5.19. What is the quotient group of D_{2n} with respect to the subgroup generated by reflection?

Exercise 5.20. Suppose G is an abelian group and H is a subgroup. Show that $\frac{G}{H}$ is abelian.

Exercise 5.21. Given N is a normal subgroup, prove that $g^k(N) = (gN)^k$.

Exercise 5.22. Suppose N is normal in G, show that for a subgroup H, $H \cap N$ is a normal subgroup in H.

Exercise 5.23. Show that a subgroup N is normal in G iff it is the kernel of a homomorphism from G to some group H.

6

Rings

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*.

6.1 Rings

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

Definition 6.1. *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 6.2. 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 6.3. Are the two conditions under the distributive law same?

Exercise 6.4. 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 6.5. The addition and multiplication of polynomials is defined in the same way as in regular polynomials.

Exercise 6.6. 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.

6.1.1 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 6.7. Prove that the set of units form a group under multiplication.

6.1.2 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 6.8. Prove that $1 \times 0 = 0$ in a ring.

6.1.3 Homomorphism for a ring

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

Exercise 6.9. 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.

6.1.4 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 6.10. 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 6.11. 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 6.12. *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 6.13. Prove that it is an ideal.

6.2 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 6.14. 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 6.15. 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 6.16. *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 6.17. Similarly we can define AB to be the ideal with *finite sums* of kind ab where $a \in A$ and $b \in B$.

Exercise 6.18. 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 6.19. 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 6.20. *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,*

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

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 6.21. 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.

6.3 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 6.22. 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 6.23. 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 6.24. 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 6.25. What is the problem with defining divisibility in ring?

6.4 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 6.26. *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 6.27. 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 6.28. 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.

6.5 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 6.29. 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 6.30. Prove all the above assertions.

6.6 Assignment

Exercise 6.31. Give a rule that is satisfied by Integers but need not be satisfied by rings in general.

Exercise 6.32. Find the set of units in the ring $\mathbb{Z}_8$.

Exercise 6.33. 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 6.34. Show that if $ab = 0$ for a, b in a field F then show that either $a = 0$ or $b = 0$.

Exercise 6.35. What are the units of a field?

Exercise 6.36. Show that a finite integral domain is a field.

Exercise 6.37. Show that the characteristic of a finite field is always a prime.

Exercise 6.38. Find a number n which leaves remainder 23 with 31, 2 with 37 and 61 with 73.

Exercise 6.39. 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 6.40. Find a number n which leaves remainder 3 when divided by 33 and 62 when divided by 81.

Hint: Trick question.

Exercise 6.41. 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 6.42. Show that $m\mathbb{Z}$ and $n\mathbb{Z}$ are comaximal in $\mathbb{Z}$.

7

Polynomials

You have seen polynomials many a times till now. The purpose of this lecture is to give a formal treatment to constructing polynomials and the rules over them. We will re derive many properties of polynomials with the only assumption that the coefficients arise from a ring or a field.

We are used to thinking of a polynomial (like $4x^2 + 2x + 6$) as an expression of coefficients (in $\mathbb{Z}, \mathbb{R}$ etc.) and variables (x, y etc.). Mostly the purpose is to solve equations and find out the value of the variable or indeterminate. But the polynomials are useful not just to figure out the value of the variable but as a structure itself. The values $x, x^2, \cdots$ should be thought of as placeholder to signify the position of the coefficients. Using this view lets define a *formal polynomial*.

7.1 Polynomials over a ring

A polynomial over a ring R is a formal sum $a_n x^n + \cdots + a_1 x + a_0$, where the coefficients come from the ring R. The set of all polynomials (in one variable) over a ring R are denoted by $R[x]$. The *degree* of the polynomial is the highest power of x with a non-zero coefficient.

We can define the addition and multiplication over polynomials (in $R[x]$) so as to match the definitions learned till now. Given two polynomials $a(x) = a_n x^n + \cdots + a_1 x + a_0$ and $b(x) = b_n x^n + \cdots + b_1 x + b_0$, their sum is defined as,

$$a(x) + b(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

If the degree of two polynomials is not equal, we can introduce extra zero coefficients in the polynomial with the smaller degree. For multiplication, given two polynomials $a(x) = a_n x^n + \cdots + a_1 x + a_0$ and $b(x) = b_m x^m + \cdots + b_1 x + b_0$, their product is defined as,

$$p(x) = a(x)b(x) = (a_n b_m)x^{n+m} + \cdots + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + (a_0 b_1 + a_1 b_0)x + (a_0 b_0).$$

More formally, the product is defined using distribution and the fact that $(ax^i)(bx^j) = (ab)x^{i+j}$.

Exercise 7.1. What is the degree of $a(x)b(x)$ if the degree of $a(x)$ is n and $b(x)$ is m?

Hint: It need not be $n + m$. why?

We mentioned while giving examples of rings that if R is a commutative ring then $R[x]$ is a commutative ring too. Using the definition above, the polynomials in multiple variables can be defined using induction. We can consider $R[x_1, x_2, \cdots, x_k]$ to be the ring of polynomials whose coefficients come from $R[x_1, x_2, \cdots, x_{k-1}]$.

Another definition of interest is the *monic* polynomial whose leading coefficient (non-zero coefficient of the highest degree) is 1. A polynomial is *constant* iff the only non-zero coefficient is the degree 0 one (a_0).

The most important polynomial rings for us would be $\mathbb{Z}_m[x]$ and $\mathbb{Z}[x], \mathbb{R}[x]$ etc..

Exercise 7.2. Suppose $a(x) = 2x^3 + 2x^2 + 2$ is a polynomial in $\mathbb{Z}_4[x]$, what is $a(x)^2$?

7.2 Polynomials over fields

After defining addition and multiplication we would like to define division and gcd of polynomials. It turns out that these definitions make sense when R is a field. For this section, we will assume that we are given a field F and the polynomials are in $F[x]$. We know that $F[x]$ is an integral domain since F is one.

Exercise 7.3. Show that $F[x]$ is an integral domain if F is an integral domain.

Exercise 7.4. For the remaining section, note where we use that the underlying ring of coefficients F is a field.

Theorem 7.5. *Division: Given two polynomials $f(x)$ and $g(x)$, there exist two* unique *polynomials called quotient $q(x)$ and remainder $r(x)$, s.t.,*

$$f(x) = q(x)g(x) + r(x).$$

where the degree of $r(x)$ is less than the degree of $g(x)$.

Proof. Existence: Suppose the degree of $f(x)$ is less than degree of $g(x)$ then $q(x) = 0$ and $r(x) = f(x)$. This will be the base case and we will apply induction on the degree of $f(x)$.

Say $f(x) = f_n x^n + \cdots + f_1 x + f_0$ and $g(x) = g_m x^m + \cdots + g_1 x + g_0$ with $m \leq n$. Multiply g by $f_n g_m^{-1} x^{n-m}$ and subtract it from f.

$$f(x) - f_n g_m^{-1} x^{n-m} g(x) = (f_{n-1} - g_{m-1} f_n g_m^{-1}) x^{n-m-1} + \cdots = l(x).$$

So l is a polynomial with lower degree and by induction it can be written as $l(x) = q'(x)g(x) + r(x)$. This implies $f(x) = (f_n g_m^{-1} x^{n-m} + q'(x))g(x) + r(x)$. So we can always find $q(x)$ and $r(x)$ with the condition given above. This method is called *long division* and is the usual method of dividing two numbers.

Exercise 7.6. What is the relation between the usual division between two integers you learnt in elementary classes and long division.

Uniqueness: Suppose there are two such decompositions $f = q_1 g + r_1$ and $f = q_2 g + r_2$ (notice that we have suppressed x for the sake of brevity). Then subtracting one from another,

$$0 = (q_1 - q_2)g + (r_1 - r_2).$$

Exercise 7.7. Show that this implies q and r are unique.

□

Using the division algorithm, we can define the Euclidean GCD algorithm.

Exercise 7.8. Read and understand the Euclidean gcd algorithm for two positive numbers.

Lets define *greatest common divisor (gcd)* first. Given two polynomials f, g, their greatest common divisor is the highest degree polynomial which divided both f, g. The important observation for Euclidean gcd is, if $f = gq_1 + r_1$ then

$$gcd(f, g) = gcd(g, r_1).$$

Without loss of generality we can assume that f has higher degree than g and hence r has lower degree than g and f. We can continue this process, say $g = q_2 r_1 + r_2$. Then the task reduces to finding the gcd of r_1 and r_2. Ultimately we get two polynomials, s.t., $r_n \mid r_{n-1}$. Then r_n is the gcd of f and g.

Exercise 7.9. Show that any polynomial which divides both f and g will also divide r_n mentioned above. Show that r_n divides both f and g.

From the previous exercise it is clear that r_n is one of the gcd (it divides both and has highest degree).

Exercise 7.10. Why is gcd unique?

Exercise 7.11. Imp: Show that using Euclidean algorithm for gcd, if $gcd(f, g) = d$ then there exist two polynomials p, q, s.t., $d = pf + qg$.

Lets define *primes* in the ring of polynomials. They are called *irreducible* polynomials (irreducible elements of integral domain $F[x]$). A polynomial f is *irreducible* iff it is not constant and there does NOT exist two non-constant polynomials g and h, s.t., $f = gh$.

Exercise 7.12. Given that a monic polynomial g is irreducible, show, any polynomial f is divisible by g or their gcd is 1. This property can be re-stated, any irreducible polynomial can't have a non-trivial gcd (trivial gcd: 1 or the polynomial itself).

With this definition we can start finding the factors of any polynomial f. Either f is irreducible or it can be written as gh. If we keep applying this procedure to g and h. We get that any polynomial f can be written as,

$$f = cg_1g_2 \cdots g_k.$$

Where g_i's are irreducible monic polynomials and c is a constant in the field F.

Can two such factorizations exist? It turns out, like in the case of natural numbers, this factorization is unique up to ordering of polynomials. For the contradiction, suppose there are two such factorizations $cg_1 \cdots g_k$ and $ch_1 \cdots h_l$.

Exercise 7.13. Why can we assume that the constant is the same for both factorizations?

We know that since g_1 is irreducible it can't have a non-trivial gcd with either $h = h_1 \cdots h_{l-1}$ or h_l. We will also show that it can't have gcd 1 with both. Suppose $gcd(h_l, g_1)$ is 1. Then using Euclidean gcd,

$$1 = ph_l + qg_1 \Rightarrow h = pf + qg_1h.$$

Since g_1 divides both terms on the R.H.S, it divides h. Hence the gcd of h and g_1 is g_1. So g_1 either divides h_l or $h = h_1 \cdots h_{l-1}$.

If it divides $h_1 \cdots h_{l-1}$, we can further divide it and ultimately get that g_1 divides h_i for some i. But since g_1 and h_i both are irreducible and monic, hence $g_1 = h_i$. This gives the theorem,

Theorem 7.14. *Unique factorization: Given a polynomial f it can be written in a unique way as a product of irreducible monic polynomials up to ordering.*

$$f(x) = cg_1(x)g_2(x) \cdots g_k(x)$$

Where c is a constant in F (the leading coefficient of f) and g_i's are irreducible monic polynomials.

Exercise 7.15. The order of going from division algorithm to Euclidean GCD to unique factorization is important. Where else have you seen this?

There is an easy way to find out whether a degree 1 polynomial $x - a$ divides a polynomial f or not. Substitute a in the polynomial f (we call the evaluation f(a)), if it evaluates to zero then $x - a$ divides f otherwise not. If $f(a) = 0$, we say that a is a *root* of f. The proof of this is given as an exercise.

Using the factorization theorem we can show that any polynomial of degree d can have at most d roots. The proof of this theorem is left as an exercise.

Theorem 7.16. *Given a polynomial p of degree d over a field F. There are at most d distinct roots of p.*

7.3 Field extension

Exercise 7.17. Why do we need complex numbers?

It might seem a weird question given the context. But lets look at the answer first. Mathematician didn't have the roots of polynomial $x^2 + 1$ in the field $\mathbb{R}$. So they came up with another field $\mathbb{C}$ where the solution existed.

Can we do it for other fields and other polynomials? This can be done and is known as *field extension*. Lets try to construct such a field extension.

Suppose we are given a field F and a polynomial p in it. We can look at the set of all polynomial in $F[x]$ modulo the polynomial p. This set is known as $\frac{F[x]}{(p)}$. The reason for this is that (p) is an ideal generated by polynomial p (it contains all multiples of p).

Exercise 7.18. Show that (p) is an ideal.

So $\frac{F[x]}{(p)}$ is just the quotient ring generated by the ideal (p).

A more intuitive way to understand this ring is, it is the set of polynomials in $F[x]$ assuming that two polynomials are equal if they only differ by a multiple of p. Using the division algorithm we can always reduce any polynomial f to a polynomial r, s.t., $f = qp + r$. Then by above discussion $r = f$ in $\frac{F[x]}{(p)}$. In the algebraic language, r is the representative of the additive coset of $F[x]$ containing f.

Exercise 7.19. Show that the elements of $\frac{F[x]}{(p)}$ are basically all the polynomials with degree less than $deg(p)$.

The ring $\frac{F[x]}{(p)}$ is a field iff p is irreducible (proof is left as an exercise). This field $\frac{F[x]}{(p)}$ is called the field extension of F. It is easy to see that an isomorphic copy of F is a subfield of $\frac{F[x]}{(p)}$.

The great thing is that there is a root of p in this new field. If you think for a minute the root is x !!

The field $\frac{F[x]}{(p)}$ can also be viewed as a vector space over F.

Exercise 7.20. What is the dimension of that vector space?

We are interested in these field extensions because they will help us characterize finite fields.

7.3.1 Another way to look at field extension

More general way to define field extensions is through subfields. Suppose K is a subset of a field L, s.t., K is field itself. Then we say that K is a sub-field of L or L is an extension of K.

Suppose s is an element of L not in K. We can extend K to include s. The smallest subfield of L which contains K as well as s is called $K(s)$. We can similarly define $K(S)$, where S is a set.

Why are the two interpretations given above similar. If s was a root of an irreducible polynomial p in K then the field $K(s)$ is precisely $\frac{K[x]}{(p)}$. All the elements of $K(s)$ can be viewed as polynomials in $K[x]$ with degree less than $deg(p)$ (substituting s for x).

Exercise 7.21. Show that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \quad a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

Notice that complex numbers can be viewed as $\mathbb{R}(i)$ or as $\frac{\mathbb{R}[x]}{x^2+1}$.

Suppose L is a field extension of K. Then L can be seen as a vector space over K. The dimension of the vector space is known as the *degree* of the extension.

Note 7.22. You might have seen vector spaces over reals and complex numbers. They can be defined over arbitrary field F by assuming that the coefficients (scalars) come from F and any addition and multiplication of scalars can be done in accordance with the field.

Exercise 7.23. What is the degree of extension $\frac{K[x]}{p}$.

Note that the subfield perspective of field extension is more general than the field extension using polynomials. Reals are an extension of rationals. It can be shown that such an extension cannot be obtained by any irreducible polynomial over rationals.

7.4 Assignment

Exercise 7.24. Write a program to compute the coefficient of x^i in $a(x)b(x)$ given two polynomials $a(x)$ and $b(x)$.

Exercise 7.25. Compute the product of $7x^3 + 2x^2 + 2x + 4$ and $2x^2 + 5x + 1$ in $\mathbb{Z}_{14}$.

Exercise 7.26. Show that in $\mathbb{Z}_p$ (p is a prime), $(x + y)^p = x^p + y^p$.

Exercise 7.27. Show that if R is an integral domain then so is $R[x]$.

Exercise 7.28. Show that $f(x)$ in $F[x]$ has an inverse iff $f(x)$ is a constant polynomial (zero excluded).

Exercise 7.29. Find out the quotient and remainder when $x^3 + 5x^2 + 2x + 3$ is divided by $x^2 + 1$ in $\mathbb{Z}_7$.

Exercise 7.30. If F is a field, is $F[x]$ also a field?

Exercise 7.31. What is the gcd of $x^n + 1$ and $x^m - 1$ in $\mathbb{Z}_2[x]$.

Exercise 7.32. Show that $x - a$ divides f iff $f(a) = 0$.

Exercise 7.33. Hard: Prove that the ring $\frac{F[x]}{(p)}$ is a field iff p is irreducible.

Exercise 7.34. Prove the theorem 7.16.

8

Finite Fields

We have learnt about groups, rings, integral domains and fields till now. Fields have the maximum required properties and hence many nice theorems can be proved about them. For instance, in previous lectures we saw that the polynomials with coefficients from fields have unique factorization theorem.

One of the important sub case of fields is when they are finite. In this case the fields can be completely characterized up to isomorphism and have lot of applications in computer science. We will cover the characterization and an application in these lecture notes.

8.1 Characteristic of a field

We have seen how the characteristic of a ring was defined.

Exercise 8.1. What is the characteristic of a ring?

Since field is a special case of rings, the definition can be applied to fields too. The characteristic of a field F is the minimum $n \in \mathbb{N}$, s.t., $n1 = 0$. Here $n1$ denotes the addition of multiplicative identity n times,

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}.$$

In general, the characteristic might not exist for field (say $\mathbb{R}$). In that case we say that characteristic is zero. For the case of finite field though, the characteristic is always a positive number. Why?

Suppose n is a characteristic of a finite field. If n is composite, say $n = pq$, then $(p1)(q1) = 0$. But F does not have a zero divisor (it is a field) and hence either $p1 = 0$ or $q1 = 0$, establishing contradiction. So we get the theorem,

Theorem 8.2. *The characteristic of a finite field is always a prime.*

Note 8.3. $p1 = 0$ implies that $pf = 0$ for all $f \in F$, the proof is given as an exercise.

How does a field with characteristic p looks like? We can look at the additive structure. It turns out that it can be seen as a vector space over $\mathbb{Z}_p$.

Exercise 8.4. Review the definition of a vector space over a field.

Theorem 8.5. *A finite field F of characteristic p is a vector space over $\mathbb{Z}_p$. Hence, if there are r basis elements then $|F| = p^r$.*

Proof. Define nf to be $\underbrace{f + f + \cdots + f}_{n \text{ times}}$. From the previous discussion, the only relevant values of n are $\{0, 1, \cdots, p-1\}$.

Let us look at the set generated by $S = \{f_1, f_2, \cdots, f_k\}$. We call it the *span*,

$$span(S) = \{n_1 f_1 + n_2 f_2 + \cdots + n_k f_k : \ n_i \in \{0, 1, \cdots, p-1\} \ \forall i\}.$$

Exercise 8.6. Show that $span(S)$ is the smallest additive group containing S.

Clearly one set exist for which span is the entire field (the field itself).

Exercise 8.7. Show that F is a vector space over $\mathbb{Z}_p$.

Say a basis $B = \{b_1, b_2, \cdots, b_r\}$ is the *minimal* set of elements such that $span(B) = F$. We have assumed that B has r elements. Then,

$$span(B) = \{n_1 b_1 + n_2 b_2 + \cdots + n_r b_r : \ n_i \in \{0, 1, \cdots, p-1\} \ \forall i\}.$$

We claim that no two elements of the above set are same. If they are then some element of B can be written as a linear combination of others, violating the minimalness of B. Hence $span(B)$ has no duplicates and it is equal to F. So the cardinality of F is p^r.

□

Note 8.8. The theorem shows that as an additive group, a field of size p^r, is isomorphic to $(\mathbb{Z}_p)^r$.

By the previous theorem we have proved that every finite field has characteristic some prime p and number of elements are p^r, some power of its characteristic. Hence the number of elements in a finite field can only be a prime power.

Does there exist a finite field for every prime power. Clearly for every p, $\mathbb{Z}_p$ is a field.

8.1.1 Finite fields of order p^r

To construct fields of cardinality p^r, we use the concept of field extension. Suppose g is an irreducible polynomial in $\mathbb{Z}_p$. Then we know that $\frac{\mathbb{Z}_p[x]}{(g)}$ is a field (from field extensions).

Exercise 8.9. Show that $\frac{\mathbb{Z}_3[x]}{x^2+1}$ is a field. What is its cardinality? What is the characteristic?

It is clear that in such a field $p1 = 0$. That shows that characteristic of the field is p. The different elements of this field are all the remainder polynomials modulo g. In other words, all the polynomials of degree $deg(g) - 1$ with coefficients from $\mathbb{Z}_p$. So the number of elements in this field are $p^{deg(g)}$.

This shows that to construct a finite field of size p^r, we need to find an irreducible polynomial of degree r. It is known that such an irreducible polynomial always exist. The proof of this statement will not be covered in this class.

So there always exist at least one field of size p^r. It can actually be shown that all such fields of size p^r are isomorphic and we call them $\mathbb{F}_{p^r}$. For $r = 1$, this field is $\mathbb{Z}_p$, we will also call it $\mathbb{F}_p$.

Exercise 8.10. What is the difference between vector space $\mathbb{Z}_3^2$ and field $\frac{\mathbb{Z}_3[x]}{x^2+1}$?

We won't prove that there exist a unique field of size p^r up to isomorphism. But we will provide a partial justification. We have seen that the additive group of any field of size p^r is isomorphic to $(\mathbb{Z}_p)^r$. In the next section we will show that their multiplicative group is also isomorphic to $\mathbb{Z}_{p^r-1}$ (it is cyclic). So for any two finite fields of same size, their additive groups and multiplicative groups are isomorphic.

Exercise 8.11. Why is this a partial and not full proof that two fields of the same size are isomorphic?

8.1.2 Primitive element

We need to show that the multiplicative group of any field is cyclic. That means, there exist an element $f \in F$, s.t., the order of f is $|F| - 1$ (why did we subtract 1?). Such an element generates the whole group $F - \{0\} = \{f^0, f^1, \cdots, f^{|F|-2}\}$.

Definition 8.12. *Primitive element: An element f of F which generates the multiplicative group of the field F is called the* primitive element *of F.*

To show that any field's multiplicative group is cyclic, we just need to show the existence of a primitive element.

Theorem 8.13. *For any finite field F, there always exist a primitive element of F.*

Proof. Lets call the multiplicative group $F^* = F - \{0\}$ and $|F^*| = n$. Since F^* has order n, for all elements x of F^*,

$$x^n - 1 = 0$$

So there are exactly n roots of the above equation (why exactly n?).

For any element x, the order d divides n, hence x is a solution of $p(d) = x^d - 1$ for some $d \mid n$. Notice that the polynomial $p(d)$ has at most d roots.

For the sake of contradiction, suppose there are no primitive elements. Then every element has order strictly less than n. We would like to show that there are not enough roots (n) for the polynomial $x^n - 1$.

So we would like to show,

$$\sum_{d<n, d|n} d < n \tag{8.1}$$

Note 8.14. There is a strict inequality $d < n$ in the summation index as well as the inequality.

Exercise 8.15. Show that this is not true for some n.

The reason why the above strategy does not work is that we are counting lot of elements multiple times. A solution of $p(d)$ will be a solution of $p(2d), p(3d), \cdots$. There is a decent chance that some of numbers $2d, 3d, \cdots$ might be divisors of n too.

So say $e(d)$ is the number of elements with order *exactly* d. Hence instead of Eq. 8.1, the contradiction will be shown by proving the equation,

$$\sum_{d<n, d|n} e(d) < n \tag{8.2}$$

This equation follows from the following two claims. The proof of first one is left as an exercise, other will be proved here.

Note 8.16. $\phi(d)$ is number of elements co-prime (gcd 1) to d.

Claim. For a number n, $\sum_{d|n} \phi(d) = n$.

Proof hint: For any number $k \leq n$, look at $gcd(k, n)$ and $\frac{k}{gcd(k,n)}$.

Claim. If there exist an element of order d then $\phi(d) = e(d)$.

Proof. Suppose the element with order d is x. Then the d roots for $x^d - 1$ are precisely $x^0, x^1, \cdots, x^{d-1}$ (these are d roots and there are at most d roots). The order of x^k is $\frac{d}{gcd(d,k)}$.

Exercise 8.17. Suppose the order of x in a group G is d. Show that for x^k, the order is $\frac{d}{gcd(d,k)}$.

Hence the elements with order d are precisely x^k, s.t., $gcd(d, k) = 1$. So $e(d) = \phi(d)$.

□

Using the claims,

$$n = \sum_{d|n} \phi(d) > \sum_{d|n} e(d).$$

The inequality follows because $e(d) \leq \phi(d)$ and we have assumed $e(n) = 0$. So the equation 8.2 follows from non-existence of primitive element and hence we get the contradiction.

Note 8.18. By definition of $e(d)$, $\sum_{d|n} e(d) = n$. Hence there should be equality in the above equation. That means there are exactly $\phi(d)$ elements of order d in a field n where $d \mid n$. Specifically, there are $\phi(n)$ primitive elements for a field F with size $n+1$.

□

Since $\mathbb{Z}_p$ is a field, by previous theorem, $\mathbb{F}_p = \mathbb{Z}_p$ is cyclic as a multiplicative group. This can be generalized to show that even $\mathbb{Z}_{p^k}^\times$ is cyclic.

Exercise 8.19. Show that $\mathbb{Z}_{p^k}^\times$ is NOT isomorphic to the multiplicative group of $\mathbb{F}_{p^k}$ for $k > 1$.

Theorem 8.20. *If $n = p^k$ for some power k of an odd prime p then $G = \mathbb{Z}_n^\times$ is cyclic.*

Note 8.21. This is not true for even prime, we have seen that $\mathbb{Z}_8^\times$ is not cyclic.

Exercise 8.22. Find out where did we use the fact that p is odd.

Proof. Assume that $t = p^{k-1}(p-1)$, the order of the group G.

We know that $\mathbb{F}_p$ is cyclic and hence have a generator g. We will use g to come up with a generator of G. First notice that,

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p \neq g^{p-1} \mod p^2.$$

So either $(g+p)^{p-1}$ or g^{p-1} is not $1 \mod p^2$. We can assume the latter case, otherwise replace g by $g+p$ in the argument below.

So $g^{p-1} = 1 + k_1 p$ where $p \nmid k_1$. So using binomial theorem,

$$g^{p(p-1)} = (1 + k_1 p)^p = 1 + k_2 p^2.$$

Where $p \nmid k_2$

Exercise 8.23. Continuing this process, show that,

$$g^{p^{e-1}(p-1)} = 1 + k_e p^e,$$

with $p \nmid k_e$.

From the previous exercise $g^t = 1 \mod p^k$ but $g^{t/p} \neq 1 \mod p^k$. The only possible order of g then is $p^{k-1}d$ where d is a divisor of $p-1$ (because the order has to divide t, Lagrange's theorem).

If the order is $p^{k-1}d$, then

$$g^{p^{k-1}d} = 1 \mod p^k = 1 \mod p.$$

But $g^p = g \mod p$ (why?). That implies $g^d = 1 \mod p$. Since $p-1$ is the order of g modulo p (g is the generator), implies $d = p-1$. Hence proved.

□

8.2 Application: The classical part of quantum algorithm for factorization

One of the most important achievements of quantum computing has been to solve factorization in polynomial time. There is no known *efficient* classical algorithm to factorize a number. The problem is easy to state, given a number n, find the factorization of n.

Note 8.24. An efficient algorithm for factorization runs in time polynomial in $\log n$, since the input size is $\log n$ (the number of bits needed to specify n).

The quantum algorithm works by reducing the problem classically to something known as the *hidden subgroup problem (HSP)*. Shor's factorization algorithm (1994) can be reduced to giving an efficient algorithm to solve HSP on a quantum computer.

The quantum algorithm for HSP is out of scope of this course. But we will present the classical reduction from factorization to HSP, a neat application of many things we learnt in this course.

8.2.1 Hidden subgroup problem (HSP)

In the hidden subgroup problem, we are given a group G and a function $f : G \to \mathbb{R}$ which *hides* a subgroup H. By hiding a subgroup means that the functions assign the same value to two elements from the same coset and different values to elements from a different coset. The subgroup H is not known and the task is to find this subgroup.

Note 8.25. For this case, we assume that a black-box is given which computes the value of a function on group elements. In practice, if we can compute the function efficiently then the algorithm for finding hidden subgroup is efficient too.

The interest in this problem is because many problems like order-finding, discrete logarithm can be thought of as HSP's over finite abelian groups. Their is a quantum algorithm for solving HSP over any finite abelian group. If we can solve HSP on non-abelian groups then it can be used to solve important problems like graph isomorphism and shortest vector problem in a lattice.

The problem of order-finding is that given an element g in a group G, find the order of g in G (smallest r, s.t., $g^r = 1$). Lets see how order-finding can be thought of as an example of HSP in $\mathbb{Z}$.

Suppose the order is r (the quantity we need to find). The set of multiples of r form a subgroup of $\mathbb{Z}$ known as $r\mathbb{Z}$. The cosets are the residue classes modulo r. Given an element $x \in \mathbb{Z}$, the function $a^x = a^{x \mod r}$ is constant on cosets and distinct on different cosets.

Exercise 8.26. Prove the above assertion.

This function can be computed efficiently (repeated squaring) and hence order-finding can be posed as a hidden subgroup problem.

Note 8.27. Above discussion shows that order-finding is an HSP over an abelian group ($\mathbb{Z}$, which is not finite). The quantum algorithm for finite abelian groups can be modified to handle this case too.

8.2.2 Factorization to order-finding

In this section we will reduce the factorization of n to order-finding in the group $\mathbb{Z}_n^\times$. Hence, complete the reduction from factorization to hidden subgroup problem.

We will first get rid of the trivial cases, it can be easily checked if the number is even or if $n = m^k$ (take the square root, cubic root etc. up to $\log n$). So it can be assumed that n is a number of type kk' where k and k' are co-prime and odd. We are interested in finding a non-trivial factor of n (not 1 or n). Once found one factor, we can repeat the procedure to find the complete factorization.

Look at the square roots of $1 \mod n$, i.e., b for which $b^2 = 1 \mod n$. Clearly there are two solutions $b = \pm 1 \mod n$. Suppose there exist a $b \neq \pm 1 \mod n$. Then $b^2 - 1$ is divisible by n and $b \pm 1$ is not. So the $gcd(b \pm 1, n)$ will give non-trivial factors of n.

The reduction from factorization to order-finding basically searches for such a b. It can be shown using Chinese remainder theorem that such a b always exists (exercise).

Exercise 8.28. In the if statement of the algorithm why didn't we check that $b = 1 \mod n$?

The only thing we need to show is that there are enough a's for which $b = a^{r/2} \neq \pm 1 \mod n$ is a square-root of $1 \mod n$.

Note 8.29. The quantum algorithm is a probabilistic algorithm, hence showing that there are enough "good" a's works.

Theorem 8.30. *Suppose n is a product of two co-prime numbers $k, k' > 1$. For a randomly chosen a, the probability that a has an even order r and $a^{r/2} \neq -1 \mod n$ is at least $1/4$.*

Check if n is even or of the form $n = m^k$;
Pick an a, s.t., $gcd(a, n) = 1$ (else we have already found a non-trivial factor of n) ;
for $i = 1, \cdots$ **do**
    Find the order of a and call it r (use the quantum algorithm for order-finding) ;
    if *r is odd or* $a^{r/2} = -1 \mod n$ **then**
        Pick another a co-prime to n ;
    else
        Found $b = a^{r/2} \neq \pm 1 \mod n$, square root of 1 ;
        Find the non-trivial factors from $gcd(b \pm 1, n)$;
        Break;
    end
end

Algorithm 1: Algorithm for factorization using order-finding

Proof. This proof is taken from the book Quantum computing and Quantum information by Nielsen and Chuang. We introduce a notation, $pow2(z)$, the highest power of 2 that divides any number z.

First we prove a lemma for a number $q = p^k$, which is a prime power. Say $m = \phi(q) = p^{k-1}(p-1)$ (exercise). By theorem 8.20, $\mathbb{Z}_q^\times$ is cyclic, say g is the generator (m is the least number, s.t., $g^m = 1 \mod q$).

Suppose $l = pow2(m)$ (m is even and hence $l \geq 1$).

Lemma 8.31. *Say, we choose a random element from $\mathbb{Z}_q^\times$. With probability $1/2$, the order r satisfies $pow2(r) = l$.*

Proof. We know that g^t has order $\frac{m}{gcd(m,t)}$. Then it can be easily seen that $pow2(r) = l$ iff t is odd.

□

Now consider the prime factorization $n = p_1^{i_1} \cdots p_s^{i_s}$. By Chinese remainder theorem,

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{i_1}}^\times \times \cdots \times \mathbb{Z}_{p_s^{i_s}}^\times.$$

So, to randomly chose a, we can pick random $a_1, \cdots, a_s$ from the respective $\mathbb{Z}_{p^i}^\times$'s. Say r_j are the orders of a_j modulo $p_j^{i_j}$.

Claim. Suppose the order r of a is odd or $a^{r/2} = -1 \mod n$. Then $pow2(r_j)$ is same for all j.

Proof. The order is odd iff all r_j's are odd. Otherwise, if $a^{r/2} = -1 \mod p_j^{i_j}$ then none of r_j divide $r/2$ (we use the fact that p_i's are not 2).

All the r_j's divide r but not $r/2$, so $pow2(r_j)$ is the same. □

From lemma 8.31, with half the probability, The order r_j of a_j will be such that $pow2(r_j) = l_j$ (where $l_j = pow2(p_j^{i_j - 1}(p_j - 1))$). Call the case when $pow2(r_j) = l_j$ as the "first" case and other the "second" case. We know that both cases happen with probability $1/2$.

Notice that l_j's only depend on n. If all l_j are equal, pick a_1's from first case and a_2 from the second case. If they are unequal, say $l_1 \neq l_2$, then pick the a_1, a_2 from the first case. So in either scenario, r_j's can't be all equal. Which implies r is even and $a^{\frac{r}{2}} \neq 1 \mod n$ (by claim). Since we have only fixed at most 2 cases out of s, the probability is at least $1/4$.

□

Hence the reduction from factorization to order finding is complete.

8.3 Assignment

Exercise 8.32. Biggs: Prove that the set of all elements of type $\underbrace{1+1+\cdots+1}_{n \text{ times}}$ form a subfield.

Exercise 8.33. If $p1 = 0$, prove that $pf = 0$ for all $f \in F$.

Exercise 8.34. Suppose in a field F, $p1 = 0$ for a prime p. Show that the characteristic of that field is p.

Exercise 8.35. Show that any field of size p is isomorphic to $\mathbb{Z}_p$.

Hint: 0 and 1 should exist in that field. Now construct the obvious isomorphism.

Exercise 8.36. Find a primitive element in field $\mathbb{F}_{23}$

Exercise 8.37. Write a program to find if a degree 2 polynomial is irreducible or not in $\mathbb{F}_p$ for a prime p.

Exercise 8.38. Construct the field $\mathbb{F}_{49}$.

Hint: Look at square roots modulo 7.

Exercise 8.39. Prove the claim 8.16.

Hint: Look at any number m less than n as $m = gcd(m, n).m'$.

Exercise 8.40. Discrete logarithm: Given an element a and a generator g in the group $G = \mathbb{Z}_m^\times$, the discrete log is the problem of finding least l, s.t., $g^l = a$. Show that it can be cast as an HSP.

Hint: Use the function $a^x g^y$ where $x, y \in \mathbb{Z}_{|G|}$.

Exercise 8.41. Show that for $n = kk'$ where k, k' are co-prime, there exist a square root of $1 \mod n$ which is not $\pm 1 \mod n$.

Exercise 8.42. If $n = p^k$, show that $\phi(n) = p^{k-1}(p-1)$.