Massachusetts Institute of Technology
6.857: Network and Computer Security
Professors Ronald L. Rivest and Yael Tauman Kalai

Handout R5
March 18, 2021
Andrés Fábrega

Recitation 5: Group Theory and Finite Fields

1 Motivation

As you may remember from lecture, a group is, very informally, simply a set of elements and a "rule"/operation that tells us how to combine two elements of the set to get a third one. Further, the elements and this rule must "behave nicely", i.e., satisfy a certain list of axioms (we will review their formal definition later). Without even noticing it, you have worked with groups before! The integers with addition is perhaps the most basic example of a group. Working with groups is nice because it gives structure to elements, and allows us to assume certain properties of these. So, working with a group is no different than hand-picking some elements that share some things in common. That way, we don't have to pay attention to anything else outside our group, and can focus our analysis on just these instead.

In cryptography, finite groups (i.e., groups where the set contains a finite number of elements) are particularly relevant. Working with a finite set is very convenient. For example, we can do things like finding upper bounds as a function of the number of possible messages, or sampling a key at random from a set. Further, using infinite fields would make our crypto-systems hard to implement in practice...

2 Group Theory Recap

Let's recall the formal definition of a group.

Definition 2.1. A *group* is a set G together with a law of composition $\cdot$ that satisfies the following axioms:

- The law of composition is **associative**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
- G contains a (unique) **identity element** 1_G such that $1_G \cdot a = a \cdot 1_G = a$ for all $a \in G$.
- Every element $a \in G$ has a unique inverse: an element b (not necessarily distinct) such that $a \cdot b = b \cdot a = 1$.

A few remarks about this definition:

(i) Note that defining the operation as a "law of composition" implicitly denotes that the group is closed under the operation: $\forall a, b \in G, \exists c \in G : a \cdot b = c$

(ii) Even thought the notation above seems very similar to multiplication, it is crucial to keep in mind that the operation can be any binary operation between elements, and it absolutely need not be multiplication. We could have used any arbitrary symbol instead of "$\cdot$" ($+$, a dollar sign, your favorite emoji, etc). Similarly, the identity element is not necessarily always the integer 1.

(iii) Groups are generally written "multiplicatively" (such as the definition above) or "additively" (using a $+$ instead of $\cdot$). This is purely out of convenience, and is mostly used whenever there is an a priori understanding of how the elements work: it would be weird to say that $7 \cdot 7 = 14$ in the group of integers with integer addition. However, this can (albeit confusing) be totally valid! Notation is mostly symbolic, but it is strongly encouraged to stick to agreed-upon conventions.

(iv) Why do we even care about associativity? It may feel a bit arbitrary to include it in the group axioms. However, this property is crucial: it makes it so that longer expressions such as $a_1 \cdot a_2 \cdot ... \cdot a_n$ are well-defined. Regardless of how we combine our elements (if we start from the left, from the right, from the middle, etc) the overall product (an element in G) will be the same.

Definition 2.2. A group $(G, \cdot)$ is *commutative* (also called Abelian) if, in addition to the group axioms, it follows that $\forall a, b \in G\ a \cdot b = b \cdot a$.

Let's go over a few (non)examples of groups to try and understand the definition better:

1. $(\mathbb{Z}, +)$. This is clearly a group. It is associative, since $(a + b) + c = a + (b + c)$. It has an identity element denoted by 0, since $a + 0 = 0 + a = a$ for any $a \in \mathbb{Z}$. Lastly, for any element a, there exists an element b such that $a + b = b + a = 0$ (namely, $-a$). So, the three group axioms are satisfied. Further, note that this is an Abelian group: $a + b = b + a$ for any two integers a, b.

   Conversely, however, $(\mathbb{Z}, \times)$ is **not** a group. It is associative since $(a \times b) \times c = a \times (b \times c)$ It has an identity element denoted by 1, since $a \times 1 = 1 \times a = a$. However, for any element a, does there exist an element b such that $a \times b = 1$? No! For, say $a = 2$, there is no other integer which we can multiply 2 by to get 1.

2. The set of invertible $n \times n$ real matrices with matrix multiplication is also a group. It is associative, since $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ for any three $n \times n$ invertible matrices A, B, C (easy to check). It has an identity element: the identity matrix I. For every A, it follows that $A \cdot I = I \cdot A = A$ (also very easy to check). Lastly, for every A, there exists a matrix B such that $A \cdot B = I$, since this is precisely the definition of being an invertible matrix. Note that, albeit trivial, it is crucial to note that the inverse of an invertible matrix is itself invertible, i.e., it is another element of the group. Further, this group is **not** Abelian, since matrix multiplication is not commutative.

   This is a very important group in abstract algebra, called the general linear group (denoted by $\mathrm{GL}_n(\mathbb{R})$.

3. $\mathbb{Z}_n^*$. This is the set of numbers between 1 and n that are coprime to n, with multiplication modulo n. We saw in class the simple argument of why this is a group.

4. The set of points on an elliptic curve over some field. This is a more advanced example outside the scope of this recitation. Feel free to come to office hours if you want to discuss this group in more detail, though!

2.1 Subgroups

Given a group $(G, \cdot)$, we can (sometimes) find a subset H of G such that it also forms a group (with the same operation). Essentially, we want to make sure that when throwing away some elements of G, we don't lose/break any of the group axioms in the process.

Definition 2.3. Let $(G, \cdot)$ be a group, and let H be a subset of G. Then, $(H, \cdot)$ is also a *subgroup* of G if:

Closure: if $a, b \in H$, then $a \cdot b \in H$.

Identity: $1_G \in H$.

Inverses: if $a \in H$, then the (unique) b such that $a \cdot b = b \cdot a = 1$ is also in H.

Note that associativity is not one of the subgroup axioms since it is already "inherited" from G: elements of H associate with all other elements of G (in particular, with those that are in H, too). Also, here we had to make closure an explicit axiom, since our law of composition is defined on G, i.e., two elements from H are guaranteed to yield an element of G, which need not be on H, too.

For example, consider the group $(\mathbb{Z}, +)$. Is $(0, 1, 2, 3, 4, 5, +)$ a subgroup of it? No! For instance, $4 + 3 = 7$ which, albeit in G, is not in H. So, it's not closed under addition. However, the group $(n\mathbb{Z}, +)$ for any $n \in \mathbb{Z}$ is indeed a subgroup. Note that the set consists of all multiplies of n. Clearly, 0 (the identity) is in this set, adding two multiples of n yields a third multiple of n, and the inverse of any multiple an is simply $-an$, i.e., another multiple of n. So, this is indeed a subgroup. Actually, there is an easy proof (but outside the scope of this class), that all subgroups of $(\mathbb{Z}, +)$ are of this form.

2.2 Order of a Group

Definition 2.4. The *order* of a group is the number of elements in the set G.

An important fact about subgroups is *Lagrange's Theorem*: the order any subgroup divides the order of the group. We will not prove it here, but its important to know it.

As was mentioned in class, groups of prime order are extremely important in cryptography, and are generally the ones we will work with. For example, as we will see next week, the DDH assumption only holds on groups of prime order. To find a group of prime order, we can start with a "safe prime" p, i.e., a prime of the form $2q + 1$. Then, we can consider the set $Q_p \coloneqq \{a^2 \ : a \in \mathbb{Z}_p^*\}$ of quadratic residues modulo p. As we showed in class, this set contains, q elements. Also, note that it is a subgroup: $1 = 1^2 \bmod p$, the product of two quadratic residues is a quadratic residue, and the inverse of a quadratic residue is also a quadratic residue. So, it is a group of prime order, as desired. For example, let $p = 7 = 2 \cdot 3 + 1$ (a safe prime). So, $\mathbb{Z}_p^*$ contains the elements $\{1, 2, 3, 4, 5, 6\}$. The quadratic residues are then $\{1^2 = 1, 2^2 = 4, 3^2 = 9 = 2, 4^2 = 16 = 2, 5^2 = 25 = 4, 6^2 = 36 = 1\} = \{1, 4, 2\}$. So, in the case $p = 7, q = 3$, the subgroup of quadratic residues has size 3, as expected. Further, this subgroup satisfies Lagrange's Theorem: it's order divides the order of the group, since 3 divides 6. Let's do another example. Let $p = 11 = 2 \cdot 5 + 1$. $\mathbb{Z}_p^*$ contains the elements $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. The quadratic residues are then $\{1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 = 5, 5^2 = 25 = 3, 6^2 = 36 = 3, 7^2 = 49 = 5, 8^2 = 9, 9^2 = 4, 10^2 = 100 = 1\} = \{1, 4, 9, 5, 3\}$. This subgroup, as expected, has size 10. How do we find these safe primes? Trial and error! Choose a random number, and test it.

Claim. *A group G of prime order p has no subgroups except $\{1\}$ and itself.*

Proof. This follows directly from Lagrange's Theorem. The order of any subgroup must divide the order of G. However, since the order is prime, the only possible orders for any subgroup are 1 and p. The only subgroup of size 1 is $\{1\}$ (since one of the subgroup axioms says that it must contain the identity).

We will now turn our attention to another important type of subgroups. Let G be a finite group, and a be an element of it. What happens if we just start applying the group operation on a multiple times? We generate a set $\{a, aa, aaa, ...\} \coloneqq \{a, a^2, a^3, ...\}$. Eventually, since the group is finite, this process must "loop" (since it can't carry on forever), and we will repeat an element we have already seen before. Let a^i and a^j be the two powers of a that first collide. Then, $a^j a^{-i} = a^{j-i} = 1$. So, we see that taking powers of a will eventually yield 1. We call this index the *order* of the element a. For example, let's take $\mathbb{Z}_7^*$ once again, and let $a = 2$. Then, $2^2 = 4, 2^3 = 1, 2^4 = 2$. We see the value 2 again, so the loop has started. Further, note that the order of 2 is 3, since this is the smaller power of 2 that yields 1. An important fact that we will use is that taking powers of any element of the group generates a new subgroup.

Claim. *The set that contains all powers of any element of a group is a subgroup.*

Proof. As mentioned above, the identity element is part of this subgroup, since there is some power of a equal to it (namely, the order of a). The set is also clearly closed under the group operation: for any integers i, j, $a^i a^j = a^{i+j}$, which is another element of the set. Lastly, it contains inverses: for any a^i, its inverse is a^{-i}, which is another power of a.

We say then that a *generates* a subgroup, which we denote by $< a >$. By definition, the size of this subgroup is the order of a. As with any subgroup, $| < a > | | |G|$, so the order of any element divides the order of the group! In our example above, $< 2 >= \{1, 2, 4\}$, the order of 2 is 3, and $3|6$. So, it follows all of our formulas. Note that, when $a \neq 1$, the order of a is greater than 1. So, if G is of prime order, the subgroup generated by any $a \neq 1$ must be G itself!

Definition 2.5. A group G is *cyclic* if $\exists a \in G$ such that $< a >= G$. We call a a *generator* of G.

For example, $\mathbb{Z}_9^*$ contains the elements $\{1, 2, 4, 5, 7, 8\}$, and 2 is a generator: $< 2 >= \{1, 2, 4, 8, 16 = 7, 32 = 5\}$.

As mentioned above, a group of prime order is cyclic, and any non-unit element is a generator.

3 Using Groups

Looking ahead, we will start building public-key cryptosystems whose security depends on a particular problem being hard. However, turns out that our choice of group is crucial! A problem may be hard to solve in one group but easy to solve in another. This is due to the fact that some groups have additional structure than can exploited by an attacker. For example, next week we will see in class why DDH doesn't hold in groups of composite order since they contain non-trivial subgroups. The three main assumptions we will work with are discrete log, DDH and CDH. In all three definitions below, G is a cyclic group with generator g.

Definition 3.1. *Discrete Log Problem (DL)*: given g^x, its hard to compute x.

Definition 3.2. *Computational Diffie-Helman Problem (CDH)*: given g^x and g^y, its hard to compute g^{xy}.

Definition 3.3. *Decisional Diffie-Helman Problem (DDH)*: given g^x and g^y, g^{xy} is indistinguishable from random.

DL is the weakest, and DDH is the strongest of these assumptions (an adversary that can break can be used to break CDH which can be used to break DDH).