Chapter 0: Preliminaries

Adam Sheffer

March 28, 2016

1 Notation

This chapter briefly surveys some basic concepts and tools that we will use in this class. Graduate students and some undergrads would probably be familiar with most or all of these. Such students may prefer to skip this chapter and only refer to it when encountering an unfamiliar concept.

We use standard asymptotic notation. That is, $f(n) = O(g(n))$ implies that there exist constants c, n_0, such that for any $n \geq n_0$, we have $f(n) \leq c \cdot g(n)$. For example, $10n^2 + 1000 = O(n^2)$ holds since we can take $c = 100$ and $n_0 = 20$. Similarly, $f(n) = \Omega(g(n))$ implies that there exist constants c, n_0, such that for any $n \geq n_0$, we have $f(n) \geq c \cdot g(n)$. Finally, $f(n) = \Theta(g(n))$ implies that both $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$ hold.

The $O^*(\cdot)$-notation is similar to the $O(\cdot)$-notation, except that it ignores polylogarithmic factors. That is, $f(n) = O(g(n))$ implies that there exist a constant n_0 and c that may have polylogarithmic dependence in n, such that for any $n \geq n_0$, we have $f(n) \leq c \cdot g(n)$. For example, $10n^2 \lg^5 n \lg\lg n + 1000 = O^*(n^2)$. We define $\Omega^*(\cdot)$ and $\Theta^*(\cdot)$ in a symmetric manner. Similarly, when writing an expression of the form $O_{s,t}(\cdot)$, we mean that the hidden constant may depend on the variables s and t. For example, $10s^{100}n^2 + s^{t^{100s}} = O_{s,t}(n^2)$.

We use standard graph theoretic notation. We usually denote a graph as $G = (V, E)$. We denote a bipartite graph as $G = (V \cup U, E)$, where V and U are the two vertex sets. Given a graph $G = (V, E)$ and a vertex $v \in V$, we set $N(v) = \{u \in V : (v, u) \in E\}$ (that is, $N(v)$ is the set of *neighbors* of v). For two disjoint subsets $A, B \subset V$, we set $E(A, B) = \{(u, v) \in E : u \in A \text{ and } v \in B\}$ (that is, the set of edges that connect the two subsets).

We denote the expectation of a random variable X as $\mathbb{E}[X]$. This is to prevent confusion between expectation and sets that are denoted as E.

We will often rely on the two following inequalities.

Claim 1.1 (The Cauchy-Schwarz inequality). *Given any two sequences of real numbers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, we have*

$$\left(\sum_{j=1}^{n} a_j b_j\right)^2 \leq \left(\sum_{j=1}^{n} a_j^2\right)\left(\sum_{j=1}^{n} b_j^2\right).$$

Claim 1.2 (Hölder's inequality). *Let p and q be two positive real numbers that satisfy $1/p + 1/q = 1$. Then for any two sequences of real numbers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, we have*

$$\sum_{j=1}^{n} |a_j b_j| \leq \left(\sum_{j=1}^{n} |a_j|^p\right)^{1/p} \left(\sum_{j=1}^{n} |b_j|^q\right)^{1/q}.$$

2 Groups

A *group* $\mathcal{G}$ consists of a set and a binary operation. Abusing notation, we will usually also refer to the set as $\mathcal{G}$. We will usually denote the operation as '+', even though this might be an operation that is very different from addition. For $\mathcal{G}$ to be a group under the operation '+', it needs to satisfy the following properties:

- **Closure.** For every $a, b \in \mathcal{G}$ we have $a + b \in \mathcal{G}$.
- **Associativity.** For every $a, b, c \in \mathcal{G}$ we have $(a + b) + c = a + (b + c)$.
- **Identity element.** There exists an element $0 \in \mathcal{G}$ such that for every $a \in \mathcal{G}$ we have $a + 0 = 0 + a = a$. This element is called the *identity element*.
- **Inverse elements.** For every $a \in \mathcal{G}$ there exists an element $-a \in \mathcal{G}$ such that $a + (-a) = (-a) + a = 0$. This element is called the *inverse* of a.

Let us consider a few simple examples of groups.

- The set of integers is a group under addition. It is obviously closed and associative, the identity element is 0, and the inverse of an integer a is $-a$.
- The set of integers is not a group under multiplication. It is closed, associative, and has the identity element 1. However, most of the integers do not have an inverse. For example, no integer x satisfies $2 \cdot x = x \cdot 2 = 1$.
- The set of even integers is a group under addition. The set of odd integers is not, since it is not closed and does not contain an identity element.

- For a positive integer n, the set $\{0, 1, 2, \ldots, n-1\}$ under addition mod n is a group. The identity element is 0 and the inverse of a is $n - a$.
- The set of non-zero rational numbers $\mathbb{Q} \setminus \{0\}$ is a group under multiplication. It is obviously closed and associative, the identity element is 1, and the inverse of a is $1/a$.
- The set of real numbers $\mathbb{R}$ under standard addition is a group. The set $\mathbb{R} \setminus \{0\}$ is a group under multiplication.

By using inverse elements we can define the inverse operation, denoted as '-'. Specifically, given a group $\mathcal{G}$ and $a, b \in \mathcal{G}$, we define $a - b$ as $a + (-b)$ (as before, the notation '-' might be a bit misleading since this operation might be very different from subtraction). Notice that being a group under '+' does not necessarily imply being a group under '-'. For example, while $\mathbb{Q} \setminus \{0\}$ is a group under multiplication, it is not a group under the inverse operation of division.

Let $\mathcal{G}$ be a group. A *subgroup* $\mathcal{G}'$ of $\mathcal{G}$ is a group under the same operation as $\mathcal{G}$ and with a subset of the elements $\mathcal{G}' \subset \mathcal{G}$. For example, the even integers under addition is a subgroup of the group of integers under addition. The set of integers that are divisible by four is in turn a subgroup of the group of even integers (both under addition).

Claim 2.1. *Let $\mathcal{G}$ be a group and let $A \subset \mathcal{G}$ be closed under the inverse operation '-' (that is, for any $a, b \in A$ we have $a - b \in A$). Then A is a subgroup of $\mathcal{G}$ (under the original operation '+').*

Proof. We need to prove that A satisfies the four basic properties of a group. First, since $\mathcal{G}$ is associative under '+' we have that A is associative under '+'. Consider an element $a \in A$ and note that by definition $a - a \in A$. Since $a - a$ is the identity element 0, we get that $0 \in A$.

For any $a \in A$, we have that $0 - a \in A$. By the definition of the identity element, $0 - a$ is the inverse of a. That is, for any $a \in A$, the inverse element $-a$ is also in A. Finally, if $a, b \in A$ then by the inverse property $-b \in A$. By the definition of A we have $a - (-b) \in A$, so $a + b \in A$. This establishes that A has the closure property and completes the proof. □

A group $\mathcal{G}$ is said to be *abelian* or *commutative* if for every $a, b \in \mathcal{G}$ we have $a + b = b + a$. All of the groups there were mentioned above are abelian, and these lecture notes will only deal with abelian groups. As an example of a non-abelian group, consider the set of $n \times n$ matrices with entries in $\mathbb{R}$ and a determinant of 1. This set is a group under standard matrix multiplication. One can verify that matrix

multiplication is associative, that the product of two $n \times n$ matrices with determinant 1 results in an $n \times n$ matrix with determinant 1, that the identity element is the $n \times n$ identity matrix, and that any matrix with a non-zero determinant has an inverse. However, this group is not abelian. For example, we have

$$\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 19 & 8 \\ 26 & 11 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 23 & 16 \\ 10 & 7 \end{pmatrix}.$$

Given a group $\mathcal{G}$ and $a \in \mathcal{G} \setminus \{0\}$, the *order* of a is the smallest positive integer k that satisfies

$$\overbrace{a + a + \cdots + a}^{k \text{ times}} = 0$$

(where 0 is the identity element of $\mathcal{G}$). For example, consider the group $\{0, 1, 2, \ldots, n-1\}$ under addition mod n, where n is an even integer larger than 2. In this group the element 1 has an order of n and the element 2 has an order of $n/2$. In the group of integers under standard addition, every non-identity element has an infinite order.

Let H be a subgroup of an abelian group $\mathcal{G}$. The *coset* of H with respect to an element $a \in \mathcal{G}$ is $a + H = \{b \in \mathcal{G} : b = a \cdot h \text{ for some } g \in H\}$. Notice that when $a \in H$ we get $a + H = H$. As an example, let $\mathcal{G}$ be the set of integers under standard addition and let H be the subgroup of even integers. Then the coset of h with respect to the element $1 \in \mathcal{G}$ is the subset of odd integers. Notice that $1 + H$ is not a subgroup.[1]

Consider two groups $\mathcal{G}_1$ and $\mathcal{G}_2$ under the respective operations $+_1$ and $+_2$. The *direct product* $\mathcal{G}_1 \times \mathcal{G}_2$ is the set $\mathcal{G}_1 \times \mathcal{G}_2$ under the following operation '+'. Given $a_1, b_1, \in \mathcal{G}_1$ and $a_2, b_2 \in \mathcal{G}_2$, we set $(a_1, b_1) + (a_2, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2)$.

Claim 2.2. *Consider two groups $\mathcal{G}_1$ and $\mathcal{G}_2$ under respective operations $+_1$ and $+_2$. Then $\mathcal{G}_1 \times \mathcal{G}_2$ is a group.*

Proof. Consider three elements $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$. By definition, we have $(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2)$. The closure of G_1 and G_2 implies that $(a_1 +_1 b_1, a_2 +_2 b_2) \in G_1 \times G_2$, which establishes the closure of $G_1 \times G_2$. By the associativity of G_1 and G_2, we have

$$\begin{aligned} \Big((a_1, a_2)+(b_1, b_2)\Big) + (c_1, c_2) &= \Big((a_1 +_1 b_1) +_1 c_1, (a_2 +_2 b_2) +_2 c_2\Big) \\ &= \Big(a_1 +_1 (b_1 +_1 c_1), a_2 +_2 (b_2 +_2 c_2)\Big) = (a_1, b_1) + \Big((b_1, b_2) + (c_1, c_2)\Big). \end{aligned}$$

[1] Usually one separately considers left cosets $a + H$ and right cosets $H + a$. Since we will only work with abelian groups this distinction is meaningless.

Denote the identity elements of $\mathcal{G}_1$ and $\mathcal{G}_2$ as 0_1 and 0_2, respectively. The identity element of $G_1 \times G_2$ is $(0_1, 0_2)$, since $(0_1, 0_2) + (a_1, a_2) = (a_1, a_2) + (0_1, 0_2) = (a_1, a_2)$. Finally, the inverse of (a_1, a_2) is $(-a_1, -a_2)$ (where $-a_j$ is the inverse of a_j). Indeed, $(a_1, a_2) + (-a_1, -a_2) = (0_1, 0_2)$. □

Given groups $G_1, G_2, \ldots, G_n$, the direct product $G_1 \times G_2 \times \cdots \times G_n$ is a group (by applying Claim 2.2 iteratively). For example, by taking every G_j to be the group of real numbers under addition, we obtain the real space $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$. That is, the set $\mathbb{R}^n$ is a group under coordinatewise addition.

A group that will be very useful to us is the set $\{0, 1, 2, \ldots, n-1\}$ under addition mod n (for a positive integer m). We refer to this group as $\mathbb{F}_n$. For a positive integer m, we set $\mathbb{F}_n^m = \mathbb{F}_n \times \mathbb{F}_n \times \cdots \times \mathbb{F}_n$ (m times).

For more basic details about groups, see for example [1].

References

[1] J. J. Rotman, A first course in abstract algebra, Pearson Prentice Hall, 2006.