Mathematical methods in communication

Lecture 12

Lecturer: Haim Permuter *Scribe: Osher Yaari*

I. GROUPS

In order to give an exact definition of a group, we first have to understand what a binary operation is:

Definition 1 (Binary Operation) Let S be a set. a *binary operation* $\oplus$ on S is a map $\oplus : S \times S \to S$, i.e it is a function (denoted by the symbol '$\oplus$') that takes two elements from the set S and returns another element from S.

For $a, b \in S$, we will usually denote the image of the pair (a, b) under the binary operation $\oplus$ by $a \oplus b$, instead of the usual $\oplus(a, b)$ notation for functions. Two main properties a binary operation can possess are:

Definition 2 (Associativity) A binary operation $\oplus$ on the set S is said to be *associative* if for all $a, b, c \in S$ we have that $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

Definition 3 (Commutativity) A binary operation $\oplus$ on the set S is said to be *commutative* if for all $a, b \in S$ we have that $a \oplus b = b \oplus a$.

When the operation is associative, we can write an expression such as $a \oplus b \oplus c$ without having to worry about specifying the order of the operations (using parenthesis), since any such choice would yield the same result. If in addition the operation is commutative, we may write the elements a, b, c in any order.

We are now ready for:

Definition 4 (Group) A *group* $(G, \oplus)$ is a set G together with a binary operation $\oplus$ on G such that:

1) (Closure) For every $a, b \in G$ we have that $a \oplus b \in G$
2) (Associativity) The operation $\oplus$ is associative

3) (Identity) There exist a special element $e \in G$, called the *identity* element, satisfying $a \oplus e = e \oplus a = a$ for all $a \in G$
4) (Inverse) For every $a \in G$ there exist $\tilde{a} \in G$, called the *inverse* of a, such that $a \oplus \tilde{a} = \tilde{a} \oplus a = e$.

If in addition we have:

5) (Commutativity) The operation $\oplus$ is commutative

then we say that it is an *abelian group* (or *commutative group*)

Notice that demanding property 1 (Closure) in the definition was unnecessary, since it follows directly from the fact that $\oplus$ is a binary operation on G. Nevertheless, we chose to include it there in order to emphasize that fact. Usually, the binary operation of a group is denoted by either $'\cdot'$ or $'+'$. When using multiplicative notation (i.e the $'\cdot'$ symbol) it it customary to denote the identity element by 1 and the inverse of an element a by a^{-1}. When using additive notation (i.e the $'+'$ symbol) it is customary to denote the identity element by 0 and the inverse of an element a by $-a$. Additive notation is generally used only for abelian groups, whereas multiplicative notation is used for both abelian and nonabelian groups.

Example 1 (Groups)

- The set $\mathbb{Z}$ of all integers together with the usual addition operation is an abelian group. All of the axioms can be easily verified here. Another example which is somewhat less trivial is the following:
- The set $GL(2, \mathbb{R})$ of all 2×2 invertible matrices together with the matrix multiplication operation is a group. First, multiplying two 2×2 invertible matrices results in another 2×2 matrix which is also invertible (why?), so this multiplication is indeed a binary operation. Second, matrix multiplication is an associative operation (not trivial but also not hard to verify). Third, the matrix I_2 is obviously a 2×2 invertible matrix who acts as the identity. Finally, every invertible matrix has an inverse. Notice that this group is *not* abelian - one can easily find two matrices A, B such that $A \cdot B \neq B \cdot A$ (try!).
- The set $\mathbb{Z}$ of all integers together with the usual multiplication operation is *not* a group, since property 4 (Inverse) does not hold here. For example, there is no integer

a which satisfies $2 \cdot a = 1$, and so the integer 2 does not have an inverse (actually, the only invertible elements here are 1 and -1).

- The set $\mathbb{Q}$ of all rational numbers together with the usual multiplication operation is also *not* a group, since now the number 0 does not have an inverse. However, this can be fixed:
- The set $\mathbb{Q} \setminus \{0\}$ of all rational numbers except the number 0 together with the usual multiplication operation *is* an abelian group.
- For $n \in \mathbb{N}$ we can take the set of numbers $\{0, 1, 2, \ldots, n-1\}$ (which we denote by $\mathbb{Z}_n$) together with the operation of addition mod-n. This formes an abelian group, where for example the identity here is the number 0, and the inverse of a number a is $n - a$. The same set together with multiplication mod-n will not form a group, since the number 0 is not invertible under multiplication. We can try to fix this by removing 0 from the set, just like we did with $\mathbb{Q}$:
- The set of numbers $\mathbb{Z}_n \setminus \{0\} = \{1, 2, \ldots, n-1\}$ together with multiplication mod-n forms a group if and only if n is prime (this will be proven in an exercise). For example, the multiplicative inverse of 3 in $\mathbb{Z}_7 \setminus \{0\}$ is 5, while for $\mathbb{Z}_6 \setminus \{0\}$ we have that $2 \cdot 3 = 0 \notin \mathbb{Z}_6 \setminus \{0\}$.

Definition 5 (Subgroup) Let $(G, +_G)$ be a group, and let $H \subseteq G$ be a subset of G. We denote by $+_H$ the restriction of the operation $+_G$ to H (i.e. $+_H := +_G|_{H \times H}$), and we say that $(H, +_H)$ is a *subgroup* of $(G, +_G)$ If $(H, +_H)$ forms a group on it's on.

For example, the even integers is a subgroup of the group of all integers (when the operation is, of course, addition). For simplicity, from now on we shall sometimes denote a group just by the set G without specifying the binary operation, for example when the specific operation is irrelevant or when it can be understood from the context. Let's introduce some more notations: the number of elements of a group $(G, +)$ is denoted by $|G|$, and say that the group is *finite* if $|G| < \infty$. For $g, h \in G$ we will write $g - h$ instead of $g + (-h)$ (remember that $-h$ is the inverse of h). If $g \in G$ and $n \in \mathbb{Z}$ we use the

notation

$$ng := \begin{cases} \overbrace{g+g+g\ldots+g}^{\text{n times}}, & \text{if } n > 0. \\ e, & \text{if } n = 0. \\ \overbrace{-g-g-g\ldots-g}^{\text{n times}}, & \text{if } n < 0. \end{cases} \tag{1}$$

Definition 6 (Cyclic Group) We say that a group G is *cyclic* if there exists some element $a \in G$ such that for every $g \in G$ we have that $g = na$ for some $n \in \mathbb{Z}$. In such case we say that a is a *generator* of G.

Example 2 (Cyclic Groups)

- The group $(\mathbb{Z}, +)$ is cyclic, since 1 and also -1 are generators.
- The group $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is cyclic, since 2 for example is a generator.

Definition 7 (Isomorphism of Groups) Let $(H, +_H), (G, +_G)$ be two groups. A map $\Phi : H \to G$ is called an *isomorphism* between H and G if:

1) Φ is bijective (i.e. one-to-one and onto)
2) For all $a, b \in H$ we have that $\Phi(a +_H b) = \Phi(a) +_G \Phi(b)$.

If there exists an isomorphism between two groups we say that those groups are *isomorphic*.

Theorem 1 Let G be a finite cyclic group with $n = |G|$ elements. Then G is isomorphic to the group $\mathbb{Z}_n$.

II. Fields

Definition 8 (Field) A *field* $(F, +, \cdot)$ is a set F together with two binary operations $+$ and $\cdot$ on F such that:

1) $(F, +)$ is an abelian group.
2) $(F \setminus \{0\}, \cdot)$ is an abelian group[1].
3) (Distributivity) For all $a, b, c \in F$ we have that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

[1]Strictly speaking, we should require that $(F \setminus \{0\}, \cdot|_{F\setminus\{0\}\times F\setminus\{0\}})$ is an abelian group.

Example 3

- $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}$ are all fields, with the usual addition and multiplication operations.
- The integers $\mathbb{Z}$ with the usual addition and multiplication operations are not a field, since $\mathbb{Z} \setminus \{0\}$ is not a group.
- If $p \in \mathbb{N}$ is prime, the set $\mathbb{Z}_p$ with addition and multiplication mod-p is a field. We will denote this field by $\mathbb{F}_p$.
- If $n \in \mathbb{N}$ is not prime then the set $\mathbb{Z}_n$ with addition and multiplication mod-n is *not* a field.

We say that a field is *finite* if it has a finite number of elements, just like we did with groups. Similarly, the terms *subfield* and *isomorphism of fields* are defined in an analogues way to the definitions we had for groups.

Theorem 2 If F is a finite field then there exists $m \in \mathbb{N}$ and a prime $p \in \mathbb{N}$ such that $|F| = p^m$. Conversely, for every prime $p \in \mathbb{N}$ and $m \in \mathbb{N}$ there exists a field F such that $|F| = p^m$, and this field is unique (up to isomorphism).

It follows from theorem 2 that for example one cannot find a field with 6 element (since 6 is not a power of a prime). It also tells us that if p is prime then $\mathbb{F}_p$ is essentially the only field with p elements (i.e any other field with p elements will be isomorphic to $\mathbb{F}_p$). Moreover, for every $m \in \mathbb{N}$ there is a (unique) field of size p^m, which we will denote as $\mathbb{F}_{p^m}$. Careful: the field $\mathbb{F}_{2^2} = \mathbb{F}_4$ is not the same as $\mathbb{Z}_4$ with addition and multiplication mod-4, as we have seen that the latter is not a field. It turns out that they will have a similar additive structure, but the multiplication will be very different. In order to understand how the multiplication looks like in such a field, we first have to talk about polynomials.

III. POLYNOMIALS

Definition 9 (Polynomial) Let F be a field and let m be a non-negative integer. A *non-zero polynomial* $f(x)$ of degree m over F is a formal expression

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{m-1} x^{m-1} + a_m x^m \tag{2}$$

where the coefficients $a_i \in F$ for all $0 \leq i \leq m$ and the leading coefficient $a_m \neq 0$. We also denote the degree by deg $f(x) = m$. The *zero polynomial* $f(x) = 0$ is a similar formal expression in which all of the coefficients are zero, and it's degree is defined to be $-\infty$.

Two polynomials are equal iff all of their coefficients coincide. Note that we think about a polynomial as a formal expression, and *not* as a function. To see the difference, consider the polynomial $f(x) = x + x^2$ over the field $\mathbb{F}_2$: it's easy to verify that $f(a) = 0$ for all $a \in \mathbb{F}_2$, yet $f(x)$ is clearly not the zero polynomial. The set of all polynomials over a field F is denoted by $F[x]$. We define the operations of addition($+$) and multiplication($\cdot$) of two polynomials in $F[x]$ in the same way one would normally add and multiply polynomials, where the coefficient operations are performed in F. With these definitions one can see that $(F[x], +)$ forms an abelian group, while $(F[x], \cdot)$ does not form a group since for example the polynomial x is not invertible. This situation resembles that of the integers $\mathbb{Z}$, and in fact these two structures have a few more similar properties which we will soon see.

A polynomial $g(x)$ is said to be a *divisor* of $f(x)$ if $f(x) = g(x) \cdot q(x)$ for some polynomial $q(x)$. $g(x)$ is called a *monic* polynomial if it's leading coefficient equals 1. We say that a monic polynomial $g(x)$ is a *factor* of $f(x)$ if $g(x)$ is a non-trivial divisor of $f(x)$ (i.e. it is a divisor that is not 1 and not $f(x)$ itself). A *prime* polynomial is a monic polynomial of degree ≥ 1 that has no factors. To illustrate these properties, lets look at some polynomials over $\mathbb{F}_3$:

- $f(x) = 0$: every polynomial is a divisor of 0, since $0 = g(x) \cdot 0$ for all $g(x) \in \mathbb{F}_3[x]$.
- $f(x) = 1$: $f(x)$ is monic with no factors, but deg $f(x) = 0$ so he is not prime.
- $f(x) = x$: $f(x)$ is prime.
- $f(x) = 2x$: $f(x)$ is not monic so it is not prime.
- $f(x) = x + 1$: $f(x)$ is prime. In fact every polynomial of the form $x + a$ is prime.
- $f(x) = x^3 + 1$: $f(x) = (x + 1)^3$ so $x + 1$ is a factor $f(x)$, hence $f(x)$ is not prime.
- $f(x) = x^2 + 2x + 1$: $f(x) = (x + 1) \cdot (x + 2)$ so he is not prime

- $f(x) = x^2 + 1$: by trying all possible combinations of degree 1 polynomials, we see that $f(x)$ is prime.

The prime polynomials in $\mathbb{F}[x]$ are very similar to the prime numbers in $\mathbb{Z}$. For example it can be shown that every monic polynomial has a unique factorization to prime polynomials, just like the fact that any integer > 1 has a unique factorization to prime numbers. Another property that $F[x]$ and $\mathbb{Z}$ have in common is the fact that we can do division with reminder for polynomials, the same way we do it for integers:

Theorem 3 Let $g(x)$ be a monic polynomial of degree m over some field F. For every $f(x) \in F[x]$ there exists unique $q(x), r(x) \in F[x]$ with deg $r(x) < m$ such that $f(x) = g(x) \cdot q(x) + r(x)$. $r(x)$ is called the *reminder*, and we denote it by $r(x) := f(x)$ mod-$g(x)$.

We will start by showing uniqueness. If $\tilde{r}(x), \tilde{q}(x)$ is another pair that satisfies the conditions of the theorem, it follows that:

$$g(x) \cdot q(x) + r(x) = g(x) \cdot \tilde{q}(x) + \tilde{r}(x) \Rightarrow g(x) \cdot (q(x) - \tilde{q}(x)) = \tilde{r}(x) - r(x) \qquad (3)$$

but the right-hand side of the last equation is of degree strictly less than deg $g(x)$, and so equality can occur only when $q(x) - \tilde{q}(x)$ is zero since otherwise the degree of the left-hand will be at least deg $g(x)$. But then $\tilde{r}(x) - r(x)$ is also zero, establishing uniqueness. The existence of such polynomials follows by simply using the regular polynomial division algorithm from high school, where the operations on the coefficients are done according to the rules of the field F. Notice that $g(x)$ is a divisor of $f(x)$ iff $f(x) = 0$ mod-$g(x)$. If deg $f(x) <$ deg $g(x)$ then the reminder of $f(x)$ mod-$g(x)$ is simply $f(x)$.

On the set $F[x]_{g(x)} := \{f(x) \in F[x]$:deg $f(x) <$deg $g(x)\}$ we can define the mod-$g(x)$ operations in the same way we do mod-n operations in $\mathbb{Z}_n$: To multiply two polynomials mod-$g(x)$ we simply multiply them in $F[x]$ and then take the reminder of the result mod-$g(x)$, and similarly for addition. For our purpose, the most important similarity between $F[x]$ and $\mathbb{Z}$ is the following: just like the integers mod-p formed a field when p was prime, we will see that the polynomials mod-$g(x)$ also form a field when $g(x)$ is prime.

IV. FINITE FIELD

Theorem 4 Let p be a prime number and let $g(x)$ be a prime polynomial of degree m over the finite field $\mathbb{F}_p$. Then the set $\mathbb{F}_p[x]_{g(x)}$ together with addition and multiplication mod-$g(x)$ forms a field with p^m elements.

Example 4 (The field $\mathbb{F}_4$) In order to construct a field with $4 = 2^2$ elements, we need to take the field $\mathbb{F}_2$ of two elements and a prime polynomial $g(x)$ of degree 2 over that field, and then look at $\mathbb{F}_2[x]_{g(x)}$ with addition and multiplication mod-$g(x)$. In this case, the only such polynomial is $g(x) = x^2 + x + 1$. The elements of the field are: $0, 1, x$ and $x+1$. The resulting addition and multiplication operations are presented in the following tables:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x