IERG6120 Coding for Distributed Storage Systems Lecture 6 - 29/09/2016

Group and Field

Lecturer: Kenneth Shum *Scribe: Xishi Wang*

1 Group and Field

A *group* $(G, \cdot)$ is a set, G, together with an operation $\cdot$ that combines any two elements a and b to form another element, denoted by $a \cdot b$ or ab. $(G, \cdot)$ satisfies the following group axioms.

1. Closed: $a \cdot b \in G, \forall a, b \in G$.
2. Associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in G$.
3. Identity: $\exists e \in G, e \cdot a = a \cdot e = a, \forall a \in G$.
4. Inverse: $\forall a \in G, \exists a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$, where e is the identity element.

We can show from the above axioms that the identity element is unique.
If $a \cdot b = b \cdot a$, namely, $\cdot$ is commutative, then G is called an *abelian group*.
Examples:

- $(\mathbb{R}, +)$. Real numbers form an abelian group under addition. The number 0 is the identity element.
- $(\mathbb{R}_{>0}, \cdot)$. Positive real numbers form an abelian group under multiplication. The number 1 is the identity element.
- $(\mathbb{R}^n, +)$. The set of all real vectors of dimension n is an abelina group under addition.
- $(\mathbb{Z}_m, +)$. The integers mod m is a finite abelian group under addition.
- The collection of all bijections from $\{1, 2, \ldots, n\}$ to itself form a group under composition. This is a finite group with $n!$ elements. This is a non-abelian group when $n > 2$.

A *field* $(F, +, \cdot)$ is a set, F, together with two operations $+$ and $\cdot$ that satisfies the following axioms.

1. F is an abelian group under $+$, with 0 as the additive identity.
2. $F \backslash \{0\} \triangleq F^*$ is an abelian group under $\cdot$.
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

A subset of a field $(F, +, \cdot)$ is called a *subfield* of F if it satisfied the above field axioms.
Example:

- The complex numbers $\mathbb{C}$ form a field.
- The set of real numbers is a subfield of $\mathbb{C}$.
- The set of rational numbers is a subfield of $\mathbb{R}$.

A *finite field* is a field with finitely many elements, e.g. $\mathbb{Z}_p$, where p is prime.
A *group table*, a.k.a. Cayley table, describes the structure of a finite group by arranging all the possible products of all the group's elements in a square table. For example, the group table for the additive group $(\mathbb{Z}_5, +)$ is

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The multiplicative table for the multiplicative group $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is

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

Proposition 1. *In each row/column of the group table of G, every element in G appears exactly once.*

Proof Suppose that there are two identical entry in a row of the group table of $(G, \cdot)$, say in the row corresponding to multiplication by an element a on the left. Then

$$\begin{aligned} a \cdot x &= a \cdot y \\ a^{-1} \cdot (a \cdot x) &= a^{-1} \cdot (a \cdot y) \\ (a^{-1} \cdot a) \cdot x &= (a^{-1} \cdot a) \cdot y \\ e \cdot x &= e \cdot y \\ x &= y \end{aligned}$$

This proves that all elements of G appear once in each row of the group table. □

Proposition 2. *For an abelian (commutative) group of size m, we have*

$$\forall g \in G, \quad g^m \triangleq \underbrace{g \cdot g \cdots g}_{m} = e,$$

where e is the identity element in G.

Proof Suppose $G = \{x_1, x_2, \ldots, x_m\}$.

$$\begin{aligned} x_1 \cdot x_2 \cdots x_m &= \underbrace{(g \cdot x_1) \cdot (g \cdot x_2) \cdots (g \cdot x_m)}_{\text{permutation of } x_1 \cdot x_2 \cdots x_m} \\ &= g^m \cdot (x_1 \cdot x_2 \cdots x_m) \\ \Rightarrow e &= g^m \end{aligned}$$

□

2 Algebraic Structure of Finite Fields

Definition 3. *Consider a (finite or infinite) field* $(\mathbb{F}, +, \cdot)$ *with additive identity* 0 *and multiplicative identity* 1*. If* $\sum_{i=1}^{c} 1 = \underbrace{1+1+\cdots+1}_{c} = 0$ *for some positive integer c, then the least positive integer c for which* $\sum_{i=1}^{c} 1 = 0$ *is called the characteristic of the filed, denoted as char*$(\mathbb{F})$*. Otherwise, if there is no positive number c such that* $\sum_{i=1}^{c} 1$ *is equal to 0, then we say that the characteristic of the field is zero.*

Theorem 4. *The characteristic of any finite field char*$(\mathbb{F})$ *must be a prime number.*

Proof Let q be the number of element in $\mathbb{F}$. We have $\sum_{i=1}^{q} 1 = 0$ by applying Proposition 2 to the additive group of $\mathbb{F}$. Hence, the set

$$\{m : m > 0, \sum_{i=1}^{m} 1 = 0\}$$

is not empty. Let c be the least integer in the above set.

We prove by contradiction that c is a prime number. If c is a composite number, say $c = c_1 c2$ with $c_1 < c$ and c_2, c, then by the distributive law, we have

$$\left(\sum_{i=1}^{c_1} 1\right) \cdot \left(\sum_{i=1}^{c_2} 1\right) = \left(\sum_{i=1}^{c} 1\right) = 0$$

$$\Rightarrow \sum_{i=1}^{c_1} 1 = 0 \quad \text{or} \quad \sum_{i=1}^{c_2} 1 = 0.$$

This contradicts the minimality of c. □

Theorem 5. *The size of a finite field* $\mathbb{F}$ *must be a power of its characteristic, namely,* $q = char(\mathbb{F})^k$.

Proof Let p be the characteristic of $\mathbb{F}$. Consider the set $\mathcal{A}_0 = \{1, \sum_{i=1}^{2} 1, \ldots, \sum_{i=1}^{p-1} 1, \sum_{i=1}^{p} 1\}$. If $\mathbb{F} = A_0$, then $|\mathbb{F}| = p$.

Otherwise, pick any element α_1 in $\mathbb{F} \backslash \mathcal{A}_0$. Let

$$\mathcal{A}_1 = \{x_0 \cdot 1 + x_1 \cdot \alpha_1 : x_0, x_1 = 0, 1, \ldots, p-1\}.$$

We now show that for distinct pairs (x_0, x_1) and (x_0', x_1'), the elements in $\mathcal{A}_1$ are distinct. Suppose $x_0 1 + x_1 \alpha_1 = x_0' 1 + x_1' \alpha_1$. If $x_1 = x_1'$, then $x_0 1 = x_0' 1$. This implies $(x_0, x_1) = (x_0', x_1')$. If $x_1 \neq x_1'$, we have $(x_1' - x_1)^{-1}(x_0 - x_0') = \alpha_1 \in \mathcal{A}_0$. This contradicts the choice of α_1. Hence, $|\mathcal{A}_1| = p^2$.

If $\mathbb{F} = \mathcal{A}_1$, then $|\mathbb{F}| = p^2$. Otherwise, we pick any element α_2 in $\mathbb{F} \backslash \mathcal{A}_1$ and repeat the above argument and show $|\mathcal{A}_2| = p^3$.

This process cannot go on forever because the size of the finite field is finite. Therefore, $|\mathbb{F}|$ must be a power of its characteristic. □

Exercises:

1. Let p be a prime. Prove that any group of size p is isomorphic to the additive group $\mathbb{Z}_p$.

2. Suppose that $GF(q)$ is a field of size q, for some prime power q. Show that the elements of $GF(q)$ are roots of polynomial $x^q - x$. Hence, show that $x^q - x$ can be factorized as

$$x^q - x = \prod_{\alpha \in GF(q)} (x - \alpha).$$

Prove that the sum of of all elements in $GF(q)$ is equal to 0, and product of all non-zero elements in $GF(q)$ is equal to -1. (Hint: Given a polynomial $f(x)$ of degree n, the coefficient of the term with degree $n-1$ is equal to the sum of roots, and the constant term is equal to the product of all roots times $(-1)^n$.)