CS 289 Communication Complexity
Instructor: Alexander A. Sherstov
Handout: Fields

Definitions

A *field* is a set F with two operations $+$ and $\cdot$ defined on it, such that the following properties hold.

- *Closure.* For any $a, b \in F$, one has $a + b \in F$ and $a \cdot b \in F$.
- *Associativity.* For any $a, b, c \in F$, one has $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- *Commutativity.* For any $a, b \in F$, one has $a + b = b + a$ and $a \cdot b = b \cdot a$.
- *Identities.* There is an element $0 \in F$ such that $0 + a = a$ for all $a \in F$. There is an element $1 \in F$ such that $1 \cdot a = a$ for all $a \in F$ with $a \neq 0$.
- *Inverses.* For every $a \in F$, there is an element $-a$ with $a + (-a) = 0$. For every $a \in F$ with $a \neq 0$, there exists an element a^{-1} with $a \cdot a^{-1} = 1$.
- *Distributivity.* For all $a, b, c \in F$, one has $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Shorthand notation. It is customary to abbreviate

$$ab = a \cdot b, \qquad a - b = a + (-b), \qquad \frac{a}{b} = a \cdot (b^{-1}).$$

Example. The reals $\mathbb{R}$ and the rationals $\mathbb{Q}$ are fields, with respect to usual addition and multiplication.

Example. The positive reals $\mathbb{R}^+$ are not a field because $-1 \notin \mathbb{R}^+$. The integers $\mathbb{Z}$ are not a field because $2^{-1} \notin \mathbb{Z}$.

Finite fields

A field with a finite number of elements is called a **finite field.**

Fact. For any prime p, the integers $0, 1, 2, 3, \ldots, p-1$ form a field (with addition and multiplication performed modulo p). This field is denoted $\mathbb{F}_p$.

Exercise. What are the multiplicative inverses in the field $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$? What about $\mathbb{F}_{11} = \{0, 1, 2, 3, \ldots, 10\}$?

Fact. For any prime power p^k, there exists a field F with $|F| = p^k$.