MORE ALGEBRAIC STRUCTURES

Definition. An **equivalence relation** on a set S is a subset of $S \times S$, where (a, b) is abbreviated as $a \sim b$, satisfying the following properties. Suppose $a, b, c \in S$.

reflexive: $a \sim a$
symmetric: $a \sim b$ implies $b \sim a$
transitive: $a \sim b$ and $b \sim c$ implies $a \sim c$

The set of all elements equivalent to a is its **equivalence class**, and we often write it as $[a]$ or $\overline{a}$.

Example (of equivalence relations)**.** "Equality" is an equivalence relation on any set. In the integers, having the same remainder after division by n is also an equivalence relation; it gives rise to $\mathbb{Z}_n$.

Remark. If two equivalence classes are even slightly different, then they have nothing in common. Put another way, **distinct equivalence classes are disjoint**. In addition, every element lies in some equivalence class (its own!), so the equivalence classes **cover** the set. These two criteria combine to show that the equivalence classes **partition** the set.

Definition. A **subgroup** S of a group G is a subset of G that remains a group *under the same operation.* For fixed $a \in G$, the **coset** $a + S$ is the set of all sums $a + s$, where $s \in S$ varies.

Remark. Keep in mind that we consider only abelian groups in this course. In a general group, we would define the coset aS as the set of all $a \circ s$, where $s \in S$ and "$\circ$" is the operation of G.

Fact (the Subgroup Theorem)**.** *A subset S of a group G is a subgroup if and only if $s - t \in S$ for all $s, t \in S$. (In the noncommutative context, if $st^{-1} \in S$.)*

Example (of subgroups)**.** The set $7\mathbb{Z} = \{\ldots, -7, 0, 7, 14, \ldots\}$ is a subgroup of the integers. We can see this because any two integer multiples of 7 have the form $7m$ and $7n$, and $7m - 7n = 7(m - n)$; integer subtraction is closed, so $m - n$ is an integer, so $7(m - n) \in 7\mathbb{Z}$.

More generally, let d be an integer. The set of integer multiples of d is a subgroup of $\mathbb{Z}$; we used no special property about 7 in the reasoning above, so we can see this by replacing 7 with d. We often write this subgroup as

$$d\mathbb{Z} = \{\ldots, -d, 0, d, 2d, \ldots\}.$$

Another example of a subgroup is a vector subspace S of a vector space V. Recall that V is a group under addition; any two vector $\mathbf{s}, \mathbf{t} \in S$ satisfy $\mathbf{s} - \mathbf{t} \in S$ by the properties of a vector subspace

Fact (Coset Equality)**.** *Two cosets $a + S$ and $b + S$ are equal if and only if $a - b \in S$.*

Example (of cosets)**.** The coset $\overline{3} = 3 + 7\mathbb{Z}$ consists of

$$\overline{3} = \{\ldots, -4, 3, 10, 17, \ldots\}.$$

We see that $\overline{3} = \overline{17}$ because $17 - 3 = 14 \in 7\mathbb{Z}$.

However, if the subgroup were $8\mathbb{Z}$, these cosets would *not* be equal; in fact, they'd contain completely different elements:

$$3+8\mathbb{Z}=\{\ldots,-5,3,11,19,\ldots\}$$
$$17+8\mathbb{Z}=\{\ldots,9,17,25,33,\ldots\}.$$

Remark. As you might have noticed from the example above, cosets always **partition** a group. This means membership in a coset is an equivalence relation!

Definition. We write G/S for the set of all cosets of S.

Fact (Lagrange's Theorem)**.** *Any two cosets of S have the same size. Thus, if G is a finite group and S is a subgroup of G, the partition implies that $|G|=|S|\,|G/S|$. In other words, the size of the group is the product of the size of the subgroup and the number of cosets. We can rewrite this relationship as $|G/S|=|G|/|S|$, which gives us a convenient formula for counting the distinct cosets S has in G.*

Remark. These facts gives us all the algebra we need to decode a message in an (n,k)-linear code with parity check matrix H:

- a linear code C is a subspace of $\mathbb{F}_q^n$, which makes it a subgroup of $\mathbb{F}_q^n$;
- by properties of a *partition,* every possible word received lies in some coset of C (**cover**);
- by Lagrange's Theorem, there are $q^n/q^k=q^{n-k}$ cosets of C;
- every erroneous message has the form $\mathbf{e}+\mathbf{x}$, where $\mathbf{x}$ is the intended message and $\mathbf{e}$ is some error;
- this erroneous message lies in the coset $\mathbf{e}+C$;
- we can identify all the coset leaders of minimal weight by
  - listing all *errors* of minimal weight, and
  - discarding those errors $\mathbf{e}_j$ that lie in the coset $\mathbf{e}_i+C$ of an already-computed error $\mathbf{e}_i$, and
  - properties of coset equality mean that we can determine this simply by checking whether
    - $\mathbf{e}_i-\mathbf{e}_j\in C$, which we can decide by checking whether
    - $H\left(\mathbf{e}_i-\mathbf{e}_j\right)=\mathbf{0}$.

In other words, decoding a message requires us neither to sort $\mathbb{F}_q^n$ into cosets, nor even to determine all the vectors in C! We need merely identify errors that produce distinct cosets, until we have found q^{n-k} such errors.