EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)

Lecture 15 — March 7, 2019

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Groups
- Subgroups

2 Groups

- Let G be a set. A binary operation $\circ$ on G is simply a function with domain $G \times G$.
- For $g, h \in G$, we write $g \circ h$ to represent $\circ(g, h)$.
- A *group* is a set G along with a binary operation which satisfies:
  - **Closure:** For all $g, h \in G$, $g \circ h \in G$.
  - **Existence of identity:** There exists an identity $e \in G$ such that for all $g \in G$, $e \circ g = g \circ e = g$.
  - **Existence of inverses:** For all $g \in G$ there exists an element $h \in G$ such that $g \circ h = h \circ g = e$. Such an h is called the inverse of g.
  - **Associativity:** For all $g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.
- Examples: $\mathbb{R}$ with $+$ and $\mathbb{R} \setminus \{0\}$ with $\times$ as operations. Note that $\mathbb{R}$ is not a group with subtraction as the operation.
- When the binary operation is understood, we simply call the set G a group.
- If G has a finite number of elements, we say G is a finite group and use $|G|$ to denote the *order* of the group (the number of group elements).
  - Example: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ under modulo n addition.
  - **Corollary:** There exists a group of every finite order $n \geq 1$.
- In general, instead of an operator like $\circ$ we will use *additive* or *multiplicative* notation.
  - In additive notation, the group operation between elements g, h is denoted $g + h$. The inverse of g is denoted by $-g$. We will write $h - g$ to mean $h + (-g)$. The identity of the group will be denoted by 0.
  - In multiplicative notation, the group operation between elements g, h is denoted gh. The inverse of g is denoted by g^{-1}. The identity of the group will be denoted by 1.

- The following lemma uses multiplicative notation. But that does not mean it is restricted to groups involving numbers. The lemma states that the usual "cancellation law" is valid for any group.
- **Lemma 8.13** Let G be a group and $a, b, c \in G$. If $ac = bc$, then $a = b$.
- The identity in a group G is *unique*.
- Each element g in a group has a *unique* inverse.
- For every $g \in G$, $\left(g^{-1}\right)^{-1} = g$.
- For every $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.
- A group is *abelian* if for all $g, h \in G$, $gh = hg$.
  - Example of non-abelian group: The set of one-to-one mappings of $\{x_1, x_2, x_3\}$ onto itself under composition operation.
- Cryptography typically involves finite abelian groups.

3 Subgroups

- If G is a group, a nonempty subset $H \subseteq G$ is a *subgroup* of G if H itself forms a group under the same operation associated with G.
- Example: Consider the subgroups of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.
- Every group G has the trivial subgroups G and $\{e\}$ where e is the identity of G.
- **Proposition:** A nonempty subset H of a group G is called a subgroup of G if and only if
  (i) $g + h \in H$ for all $g, h \in H$.
  (ii) $-g \in H$ for all $g \in H$.
- **Lagrange's Theorem:** If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.
  - Example: Consider the subgroups of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ again.
  - **Definition:** Let H be a subgroup of a group G. For any $g \in G$, the set $H + g = \{h + g \mid h \in H\}$ is called a *right coset* of H.
  - For abelian groups, there is only a notion of a coset as both right and left cosets are the same, i.e. $H + g = g + H$. For non-abelian groups, this is not necessarily true.
  - **Example:** $H = \{0, 3\}$ is a subgroup of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. It has right cosets
    $H + 0 = \{0, 3\}$, $H + 1 = \{1, 4\}$, $H + 2 = \{2, 5\}$,
    $H + 3 = \{0, 3\}$, $H + 4 = \{1, 4\}$, $H + 5 = \{2, 5\}$.
  - **Lemma:** Two right cosets of a subgroup are either equal or disjoint.
  - **Lemma:** If H is a finite subgroup, then all its right cosets have the same cardinality.
  - The proof of Lagrange's theorem follows from these two lemmas.

4 References and Additional Reading

- Section 8.1 from Katz/Lindell
- Sections 2.1–2.4 of *Topics in Algebra*, I. N. Herstein, 2nd edition