Number Theory & Cryptography

Written by HADIOUCHE Azouaou.

Disclaimer

This document contains the lectures given by Dr. ZAIMI.

> Some contents were added as remainders and extras for the students.
> To separate the contents of the course to actual additions or out of context information, a black band will be added by its side like the globing this comment.

Contents

Chapter 3

Group Actions

Definition 3.1 (Group Actions): *Let G be a group and $X \neq \emptyset$, we say that G acts (operates) on X if there is a homomorphism $\varphi : G \to \mathcal{S}(X)$ the group of permutations of x.*

To avoid complicated notation, we denote $\varphi(g)(x) = \varphi_g(x)$ as $g \cdot x$. Notice in this case $e \cdot x = \varphi(e)(x) = \mathrm{Id}(x) = x$ and $(g_1 g_2) \cdot x = \varphi(g_1 g_2)(x) = \varphi(g_1) \circ \varphi(g_2)(x) = g_1 \cdot (g_2 \cdot x)$.

Definition 3.2 (Group Actions): *Let G be a group and $X \neq \emptyset$ if there is a map $G \times X \to X, (g, x) \mapsto g \cdot x$ where it satisfies the following two identities for any $x \in X$, $g_1, g_2 \in G$, $e \cdot x = x$ and $g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x)$ then we say that G acts on X.*

The two previous definitions are equivalent.

Definition 3.3 (Orbit/Stabilizer): *Let G be a group acting on X (X is a G-set) and let $x \in X$, we define the following*
1. *The orbit of x as $O_x = \{g \cdot x \mid g \in G\}$.*
2. *The stabilizer of x as $S_x = \{g \in G \mid g \cdot x = x\}$.*

Proposition 3.4: *S_x is a subgroup of G.*

Proof. By definition 2, we have $e \cdot x = x$ thus $e \in S_x$. Let $g_1, g_2 \in S_x$ then $g_1 \cdot x = x$ and $g_2 \cdot x = x$, so $g_1 g_2 \cdot x = g_1 (g_2 \cdot x) = g_1 x = x$ so $g_1 g_2 \in S_x$. Also, $g_1 \cdot x = x \Rightarrow x = e \cdot x = g_1^{-1}(g_1 \cdot x) = g_1^{-1} \cdot x$ thus $g_1^{-1} \in S_x$. □

Proposition 3.5: *The relation defined on X by $x \mathcal{R} x' \Leftrightarrow x' \in O_x$ is an equivalence relation and the class of x is O_x.*

Proof. Trivial. □

Definition 3.6:
1. *If $O_x = X$ for some $x \in X$, then we say that G acts transitively on X.*
2. *If $O_x = \{x\}$, then x is said to be stable or fixed, in this case $S_x = G$.*

Proposition 3.7: *Let X be a G-set and let x, y in the same orbit, then S_x and S_y are conjugates.*

Proof. Let $y \in O_x$, then $y = gx$ for some $g \in G$. Let $h \in S_x$, then $hx = x$, $(ghg^{-1})(y) = ghx = gx = y$ therefore $gS_x g^{-1} \subseteq S_y$ in a similar way we get $g^{-1} S_y g \subseteq S_x$ by multiplying both sides by g and g^{-1} we get $S_y \subseteq g S_x g^{-1}$ which gives that $S_y = g S_x g^{-1}$. □

Proposition 3.8: *Let X be a G-set, then there is a bijection between the set of left cosets of S_x in G and O_x.*

Proof. Let $\mathcal{L}$ be the set of left cosets. Consider the function $\varphi : \mathcal{L} \to O_x, gS_x \mapsto gx$. φ is well defined and injective since $gS_x = hS_x \Leftrightarrow h^{-1}g \in S_x \Leftrightarrow h^{-1}gx = x \Leftrightarrow gx = hx \Leftrightarrow \varphi(gS_x) = \varphi(hS_x)$ and it is surjective by definition. □

Corollary 3.9: *Let G finite and let X be a G-set then $\# G = \# O_x \cdot \# S_x$.*

Proof. By Lagrange theorem, we have that $\# G = \# S_x [G : S_x]$ and by the previous proposition we have $\# G = \# S_x [G : S_x] = \# S_x \# O_x$. □

Corollary 3.10 (Class Equation): *Let G be finite and let $O_{x_1}, O_{x_2}, ..., O_{x_n}$ be the distinct orbits of G-set X then X is finite and $\# X = \sum_{i=1}^{n} \# O_{x_i}$.*

Definition 3.11 (p-Group): *Let G be a group of order p^n where p is a prime and $n \in \mathbb{N}$, G is said to be a p-group.*

A subgroup of a p-group is also a p-group by Lagrange's theorem.

Corollary 3.12 (Burnside): *The center of a p-group is a p-group.*

Proof. Let G be a p-group, $\mathcal{Z}(G)$ the center of G and consider the action on G defined by $G \times G \to G, (g, x) \mapsto gxg^{-1}$. Let $O_{x_1}, ..., O_{x_k}$ be the distinct orbits for this action. Notice that $\forall x \in X, O_x = \{x\} \Leftrightarrow \forall g \in G, gxg^{-1} = x \Leftrightarrow \forall g \in G, gx = xg \Leftrightarrow x \in \mathcal{Z}(G)$. Suppose that $\# G = p^n$, then is either $\# O_{x_i} = 1$ or $\# O_{x_i} = p^{n_i}$ and suppose that $\mathcal{Z}(G) = \{x_1, ..., x_s\}$. Thus by the class equation

$$\begin{aligned} \# G = \# X = \sum_{i=1}^{s} \# O_{x_i} + \sum_{i=s+1}^{n} \# O_{x_i} \\ p^n = s + (p^{n_{s+1}} + \cdots + p^{n_k}) \\ s = p^n - (p^{n_{s+1}} + \cdots + p^{n_k}) \end{aligned}$$

$s \geq 1$ given that $e \in \mathcal{Z}(G)$ and since p divides the RHS then it divides s so the center is a p-group. □

Corollary 3.13 (Cauchy): *Let G be a finite group and let p a prime number that divides $\# G$, then there is an element in G of order p.*

Proof. We have already proven this result for the case where G is abelian. Suppose that G is non-abelian. Consider $\# G = n$. For $n = 1$, the result is trivial. Suppose that the result is true for all non-abelian groups of order less than n. If there is a subgroup H of G whose order is divisible by p, we get the result from the induction hypothesis. So suppose that $\# H \not\equiv 0 \bmod p$ for all subgroups H of G with $H \neq G$. Consider the conjugation action $g \cdot x = gxg^{-1}$. We have that $O_x = \{»\} \Leftrightarrow x \in \mathcal{Z}(G)$. Let $O_{x_1}, ..., O_{x_r}$ be the orbits of the action where $x_1, ..., x_s$ are in $\mathcal{Z}(G)$. Then by class equation we have $\# G = s + \sum_{i=s+1}^{r} O_{x_i}$, on the other hand $\# O_{x_i} = \# G / \# S_{x_i}$, we have that $\# O_{x_i} > 1$ for $x_i \notin \mathcal{Z}(G)$, p does not divide $\# S_{x_i}$ and it divides $\# G$ thus it divides $\# O_{x_i}$, it follows that p divides s and thus $p \mid \# \mathcal{Z}(G)$ which is a contradiction. □