PMATH348 — Fields and Galois Theory

Classnotes for Winter 2019

by

Johnson Ng

BMath (Hons), Pure Mathematics major, Actuarial Science Minor

University of Waterloo

Table of Contents

List of Definitions

List of Theorems

Preface

This is a 3 part course; it is separated into

1. **Sylow's Theorem**

   which is a leftover from group theory (PMATH 347). It has little to do with the rest of the course, but PMATH 347 was a course that is already content-rich to a point where Sylow's Theorem gets pushed into the later course that is this course.

2. **Field Theory**

   is a somewhat understood concept from ring theory, where we learned that it is a special case of a ring where all of its elements have an inverse.

3. **Galois Theory**

   is the beautiful theory from the French mathematican Évariste Galois that ties field theory back to group theory. This allows us to reduce certain field theory problems into group theory, which, in some sense, is easier and better understood.

Part I

Sylow’s Theorem

1 Lecture 1 Jan 07th

1.1 Cauchy's Theorem

Recall Lagrange's Theorem.

Theorem 1 (Lagrange's Theorem)

If G is a finite group and H is a subgroup of G [1]*, then $|H| \mid |G|$* [2]*.*

The full converse is not true.

Example 1.1.1

Let $G = A_4$, the **alternating group** of 4 elements. Then $|G| = 12$ [3]. We have that $6 \mid 12$. We shall show that G has no subgroup of order 6.

Suppose to the contrary that $H \leq G$ such that $|H| = 6$. Let $a \in G$ such that $|a| = 3$ [4] There are 8 such elements in G [5]. Note that the **index**[6] of H, $|G : H|$, is $\frac{|G|}{|H|} = 2$.

Now consider the **cosets** H, aH and a^2H. Since $|G : H| = 2$, we must have either

- $aH = H \implies a \in H$;
- $aH = a^H \overset{\text{'multiply' } a^{-1}}{\Longrightarrow} H = aH \implies a \in H$; or
- $a^2H = H \overset{\text{'multiply' } a}{\Longrightarrow} H = aH \implies a \in H$.

Thus all 8 elements of order 3 are in H but $|H| = 6$, a contradiction. Therefore, no such subgroup (of order 6) exists.

[1] I shall write this as $H \leq G$ from hereon.

[2] This just means $|H|$ divides $|G|$.

[3] Recall that the symmetric group of 4 elements S_4 has order $4! = 24$, and an alternating group has half of its elements.

[4] i.e. the order of a is 3. This is a **trick**.

[5] This shall be left as an exercise.

Exercise 1.1.1

Prove that there are 8 elements in G that have order 3.

[6] The index of a subgroup is the number of unique cosets generated by H.

Our goal now is to establish a partial converse of Lagrange's Theorem. To that end, we shall first lay down some definitions.

Definition 1 (p-Group)

*Let p be prime. We say that a group G is a **p-group** if $|G| = p^k$ for some $k \in \mathbb{N}$. For $H \leq G$, we say that H is a p-subgroup of G if H is a p-group.*

Definition 2 (Sylow p-Subgroup)

*Let G be a group such that $|G| = p^n m$ for some $n, m \in \mathbb{N}$, such that $p \nmid m$. If $H \leq G$ with order p^n, we call H a **Sylow p-subgroup**.*

Recall Cauchy's Theorem for abelian groups[7].

Theorem 2 (Cauchy's Theorem for Abelian Groups)

If G is a finite abelian group, and p is prime such that $p \mid |G|$, then $|G|$ has an element of order p.

Definition 3 (Stabilizers and Orbits)

*Let G be a finite group which acts on a finite set X [8]. For $x \in X$, the **stabilizers** of x is the set*

$$\operatorname{stab}(x) := \{g \in G : gx = x\} \leq G.$$

The orbits of x is a set

$$\operatorname{orb}(x) := \{gx : g \in G\}.$$

Note

One can verify that the function $G/\operatorname{stab}(x) \to \operatorname{orb}(x)$ such that

$$g \operatorname{stab}(x) \mapsto gx$$

[7] In the course I was in, we were introduced only to the full theorem and actually went through this entire part. See notes on PMATH 347.

[8] Recall that a group action is a function $\cdot : G \times X \to X$ such that

1. $g(hx) = (gh)x$; and
2. $ex = x$.

is a bijection.

☕ Theorem 3 (Orbit-Stabilizer Theorem)

Let G be a group acting on a set X, and for each $x \in X$, $\mathrm{stab}(x)$ and $\mathrm{orb}(x)$ are the stabilizers and orbits of x, respectively. Then

$$|G| = |\mathrm{stab}(x)| \cdot |\mathrm{orb}(x)| .$$

Moreover, if $x, y \in X$, then either $\mathrm{orb}(x) \cap \mathrm{orb}(y) = \emptyset$ or $\mathrm{orb}(x) = \mathrm{orb}(y)$.

The theorem is actually equivalent to Proposition 45 in the notes for PMATH 347. However, feel free to...

Exercise 1.1.2

prove ☕ Theorem 3 as an exercise.

Consequently, we have that

$$|X| = \sum |\mathrm{orb}(a_i)| ,$$

where a_i are the distinct orbit representatives. Letting

$$X_G := \{x \in X : gx = x, g \in G\},$$

we have...

☕ Theorem 4 (Orbit Decomposition Theorem)

$$|X| = |X_G| + \sum_{a_i \notin X_G} |\mathrm{orb}(a_i)| .$$

Index