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].

[1] I shall write this as $H \leq G$ from hereon.
[2] This just means $|H|$ divides $|G|$.

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.

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

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 $\frac{|G|}{|H|} = 2$.

[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.

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

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

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

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].

[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.

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*

$$\mathrm{Stab}(x) := \{g \in G : gx = x\} \leq G.$$

The orbits of x is a set

$$\mathrm{Orb}(x) := \{gx : g \in G\}.$$

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

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

Note

One can verify that the function $G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)$ such that

$$g\,\mathrm{Stab}(x) \mapsto gx$$

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)

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

2 Lecture 2 Jan 09th

2.1 Sylow Theory

From the Orbit Decomposition Theorem, one special case is when G acts on $X = G$ by conjugation.

Corollary 5 (Class Equation)

From Theorem 4, if $X = G$, we have

$$\begin{aligned} |G| &= |Z(G)| + \sum |\text{Orb}(a_i)| \qquad \text{(non-central } \uparrow\text{)} \\ &= |Z(G)| + \sum [G : \text{Stab}(a_i)] \text{ by } \textit{Orbit} - \textit{Stabilizer} \\ &= |Z(G)| + \sum [G : C(a_i)], \end{aligned}$$

*where $C(a_i)$ is called the **centralizers** of G.*

Theorem 6 (First Sylow Theorem)

Let G be a finite group, and let $p \mid |G|$ such that p is prime. Then G contains a Sylow p-subgroup.

Proof

We proceed by induction on the size of G. If $|G| = 2$, then $p = 2$, and so G is its own Sylow p-subgroup [1].

Consider a finite group G with $|G| \geq 2$. Let p be a prime that divides $|G|$, and assume that the desired result holds for smaller groups.

[1] A 2-cycle is a Sylow p-group.

Let $|G| = p^n m$, where $n, m \in \mathbb{N}$, and $p \nmid m$.

Case 1: $p \mid |Z(G)|$ By Theorem 2, $\exists a \in Z(G)$ such that $|a| = p$. Since $\langle a \rangle \subsetneq Z(G)$, we have that

$$\langle a \rangle \triangleleft G \text{ and } |\langle a \rangle| = p.$$

[2] Notice that the group $G/\langle a \rangle$ is a group that has a lower order than G, and so by IH, $\exists \overline{H} \leq G/\langle a \rangle$ such that $\overline{H}$ is a Sylow p-subgroup of $G/\langle a \rangle$. Note that if $n = 1$. then $\langle a \rangle$ itself is the Sylow p-subgroup. WMA $n > 1$. We have that $|H| = p^{n-1}$. By correspondence,

$$\overline{H} = H/\langle a \rangle,$$

where $H \leq G$. By comparing the orders, we have

$$p^{n-1} = \frac{|H|}{p} \implies |H| = p^n.$$

Therefore H is a Sylow p-subgroup of G.

Case 2: $p \nmid Z(G)$ By the class equation, notice that

$$p^n m = |G| = |Z(G)| + \sum [G : C(a_i)], \tag{2.1}$$

and the summation cannot be 0 or p would otherwise divide $Z(G)$.

> *Since p divides the LHS of Equation (2.1) and not $|Z(G)|$, and the sum is nonzero, we must have that $\exists a_i \in G$ such that $p \nmid [G : C(a_i)]$. This implies that $p^n \mid |C(a_i)|$.*

Since $a_i \notin Z(G)$, we have $|C(a_i)| \leq |G|$. Thus by IH, $C(a_i)$ has a Sylow p-subgroup, which is also a Sylow p-subgroup of G. □

Corollary 7 (Cauchy's Theorem)

If p is prime and $p \mid |G|$, then G has an element of order p.

Proof

WLOG, WMA $|G| = p^n m$, where $n, m \in \mathbb{N}$ and $p \nmid m$. By Theorem 6, $\exists H \leq G$ such that H is a Sylow p-subgroup. Take $a \in H \setminus \{e\}$. Then $|a| = p^k$ for some $k \leq n$.

[2] This feels like a struck of genius. Let's break it down and find some way that makes it easier to remember. We want to find $H \leq G$ such that $|H| = p^n$. We have $|\langle a \rangle| = p$. We want to be able to use the **Correspondence Theorem**, so we should adjust our materials to fit that mold: since $|\langle a \rangle| = p$, notice that

$$\frac{|G|}{|\langle a \rangle|} = p^{n-1} m.$$

This is a smaller group than G, and so IH tells us that it has a Sylow p-subgroup, say $\overline{H}$. By the Correspondence Theorem, we may retrieve H.

This highlighted part requires clarification.

Let $b = a^{p^{k-1}}$. Notice that $b \neq e$, or it would contradict the definition of an order (for a). Then $b^p = \left(a^{p^{k-1}}\right)^p = a^p = e$. Therefore $|b| = p$ and $b \in G$. □

Definition 4 (Normalizer)

Let G be a group, and $H \leq G$. The set

$$N_G(H) = \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\}$$

*is called the **normalizer** of H in G.*

Exercise 2.1.1

Verify that $N_G(H)$ is the largest subgroup of G that contains H as a normal subgroup.

Proof

It is clear by definition of a normalizer that $H \triangleleft N_G(H)$.

Suppose there exists $N_G(H) < \tilde{H} \leq G$ such that $H \triangleleft \tilde{H}$. Let $h \in \tilde{H} \setminus N_G(H)$. But since $H \triangleleft \tilde{H}$, we have

$$hHh^{-1} = H,$$

which implies that $h \in N_G(H)$, a contradiction. Therefore $N_G(H)$ is the largest subgroup that contains H as a normal subgroup.

Before proceeding with the Sylow's next theorem, we require two lemmas.

Lemma 8 (Intersection of a Sylow p-subgroup with any other p-subgroups)

Let G be a finite group and p a prime such that $p \mid |G|$. Let $P, Q \leq G$ be a Sylow p-subgroup and a (regular) p-subgroup, respectively. Then

$$Q \cap N_G(P) = Q \cap P. \tag{2.2}$$

Proof

Since $P \subseteq N_G(P)$, $\subseteq$ of Equation (2.2) is done.

Let $N = N_G(P)$, and let $H = Q \cap N$. WTS $H \subseteq Q \cap P$. Since $H = Q \cap N \subseteq Q$, it suffices to show that $H \subseteq P$. Since P is a Sylow p-subgroup, let $|P| = p^n$. By Lagrange, we have that $|H| = p^m$ for some $m \leq n$. Since $P \triangleleft N$, we have that $HP \leq N$ [3]. Moreover, we have that

$$|HP| = \frac{|H|\,|P|}{|H \cap P|} = p^k$$

for some $k \leq n$. Also, $P \subset HP$, and so $n \leq k$, implying that $k = n$. Thus $P = HP$, and thus

$$H \subseteq HP = P,$$

as required. □

[3] See PMATH 347

3 Lecture 3 Jan 11th

3.1 Sylow Theory (Continued)

Lemma 9 (Counting The Conjugates of a Sylow p-Subgroup)

Let G be a finite group, and p a prime such that $p \mid |G|$. Let

- *P be a Sylow p-subgroup;*
- *Q be a p-subgroup;*
- *$K = \{gPg^{-1} \mid g \in G\}$;*
- *Q act on K by conjugation; and*
- *$P = P_1, P_2, \ldots, P_r$ be the distinct orbit representatives from the action of Q on K.*

Then

$$|K| = \sum_{i=1}^{r} [Q : Q \cap P_i] .$$

Proof

From the definition of K, and the fact that Q acts on K, we have

$$\begin{aligned}
|K| &= \sum_{i=1}^{r} |\text{Orb}(P_i)| \\
&= \sum_{i=1}^{r} |Q| \,/\, |\text{Stab}(P_i)| \quad \text{orbit-stabilizer} \\
&= \sum_{i=1}^{r} |Q| \,/\, |N_G(P_i) \cap Q| \quad \text{by the action} \\
&= \sum_{i=1}^{r} [Q : N_G(P_i) \cap Q] \quad \text{by definition} \\
&= \sum_{i=1}^{r} [Q : Q \cap P_i] \quad \text{the last lemma.}
\end{aligned}$$

□

Theorem 10 (Second Sylow Theorem)

If P and Q are Sylow p-subgroups of G, then $\exists g \in G$ such that $P = gQg^{-1}$.

Proof

Let $K = \{qPq^{-1} \mid q \in G\}$. WTS $Q \in K$. We shall also note that $|P| = p^k$ for some $k \in \mathbb{N}$.

Let P act on K by conjugation. Let the orbit representatives be

$$P = P_1, P_2, \ldots, P_r.$$

By Lemma 9, we have

$$|K| = \sum_{i=1}^{r} [P : P \cap P_i] = [P : P] + \sum_{i=2}^{r} [P : P \cap P_i] = 1 + \sum_{i=2}^{r} [P : P \cap P_i].$$

Thus

$$|K| \equiv 1 \mod p.$$

Now let Q act on K by conjugation. Reordering if necessary, the orbit representatives are

$$P = P_1, P_2, \ldots, P_s,$$

where s is not necessarily r. From here, it suffices to show that $Q = P_i$ for some $i \in \{1, 2, \ldots, s\}$. Suppose not. Then by Lemma 9,

$$|K| = \sum_{i=1}^{s} [Q : P_i \cap Q].$$

Note that it must be the case that $[Q : P_i \cap Q] > 1$, for some if not all i, for otherwise it would imply that $Q \cap P_i$ and that would be a contradiction. Then by Lagrange,

$$|K| \equiv 0 \mod p.$$

This contradicts the fact that $|K| \equiv 1 \mod p$.

This shows that $Q = P_i$ for some $i \in \{1, 2, \ldots, s\}$, and so Q is a conjugate of P. □

Note (Notation)

We shall denote n_p as the number of Sylow p-subgroups in G.

Theorem 11 (Third Sylow Theorem)

Let p be a prime, and that it divides $|G|$, where G is a group. Suppose $|G| = p^n m$, where $n, m \in \mathbb{N}$ and $p \nmid m$. Then

1. $n_p \equiv 1 \mod p$; *and*
2. $n_p \mid m$.

Proof

Let P be a Sylow p-subgroup of G, and let

$$K = \left\{ gPg^{-1} \;\middle|\; g \in G \right\}.$$

By Sylow's second theorem, $n_p = |K|$ as all the conjugates are exactly the Sylow p-subgroups. And by our last proof, we saw that $n_p \equiv 1 \mod p$.

Let G act on K by conjugation. Then by the Orbit-Stabilizer Theo-

rem,

$$|G| = |\text{Stab}(P)|\,|\text{Orb}(P)|\,.$$

Thus

$$p^n m = |N_G(P)|\, n_p. \tag{3.1}$$

Thus $n_p \mid p^n m$. Since $n_p \equiv 1 \not\equiv 0 \mod p$, we must have $n_p \mid m$. □

Remark

1. *From Equation (3.1), we have that*

$$n_p = [G : N_G(P)].$$

2. ★ *Note that*

$$n_p = 1 \iff \forall g \in G\ gPg^{-1} = P \iff P \triangleleft G.$$

*However, note that P **may be trivial**! This means that if G is simple, it does not imply that $n_p = 1$.*

Definition 5 (Simple Group)

*A group is said to be **simple** if it has no non-trivial normal subgroups.*

Example 3.1.1

Prove that there is no simple group of order 56.

Proof

Let G be a group. Note that $56 = 2^3 \cdot 7$. Then $n_7 \equiv 1 \mod 7$ and $n_7 \mid 8 = 2^3$. Thus

$$n_7 = 1 \text{ or } n_7 = 8.$$

$n_7 = 1$ By the remark above, G has a normal Sylow 7-subgroup. Thus G is not simple.

$n_7 = 8$ By Lagrange, since 7 is prime, by the Finite Abelian group structure, the distinct Sylow 8-subgroups of G intersect trivially. Therefore, there are $8 \times 6 = 48$ elements of order 7 in G. But this

implies that $56 - 48 = 8$ elements that are not of order 7. One of them is the identity, thus the remaining 7 elements must have order 2 [1]. This implies that

$$n_2 = 7 \equiv 1 \mod 2,$$

which by our remark means that G has a normal Sylow 2-subgroup. Thus G is not simple by both accounts.

[1] They cannot be of any other order as that would create a cyclic group that is not of order 2 or 7, which is impossible.

4 Lecture 4 Jan 14th

4.1 Sylow Theory (Continued 2)

Remark

1. *Let $p \neq q$ both be primes, and $p, q \mid |G|$. Let H_p and H_q be a Sylow p-subgroup and a Sylow q-subgroup of G, respectively. By Lagrange's Theorem, we must have that $H_p \cap H_q = \{e\}$. Then*

$$|H_p \cup H_q| = |H_p| + |H_q| - 1.$$

2. *Let $|G| = pm$ and $p \nmid m$, where p is prime. If H, K are Sylow p-subgroups of G with $H \neq K$, then $H \cap K = \{e\}$.*

Example 4.1.1

Note that the second remark is not true if $G = D_6$. Notice that

$$H = \langle 1, s \rangle, \quad K = \langle 1, rs \rangle$$

are both Sylow 2-subgroups of D_6 and $H \neq K$, and their intersection is trivial.

Example 4.1.2

Let $|G| = pq$ where p, q are primes with $p < q$ and $p \nmid q - 1$. Then $|G|$ is cyclic.

Proof

By the Third Sylow Theorem, $n_p \equiv 1 \mod p$ and $n_p \mid q$. Notice that $n_p = 1$, since if $n_p = q$, then $n_p \equiv 1 \mod p \implies p \mid q - 1$, contradicting our assumption. By our remark last lecture, G has a normal Sylow p-subgroup, which we shall call H_p.

On the other hand, $n_q \equiv 1 \mod q$ and $n_q \mid p$. Since $p < q$, $q \nmid p-1$, and so the same argument as before holds. Hence $n_q = 1$, and so G has a normal Sylow q-subgroup.

Since $H_p \triangleleft G$, we know that $H_pH_q \leq G$, and we notice that

$$\left|H_pH_q\right| = \frac{\left|H_p\right|\left|H_q\right|}{\left|H_p \cap H_q\right|} = pq = |G|.$$

Thus $G = H_pH_q$. Let $a, b \in G$. If a, b is either both in H_p or both in H_q, then $ab = ba$ [1]. WMA $a \in H_p$ and $b \in H_q$. By our first remark today, note that $H_p \cap H_q = \{e\}$. Then, observe that

[1] Crap, I don't remember why...

$$\underbrace{aba^{-1}}_{H_q} \overset{\uparrow}{b}^{-1} \in H_q \qquad \overset{\uparrow}{a} \underbrace{ba^{-1}b^{-1}}_{H_p} \in H_p$$
$$H_q \qquad\qquad H_p$$

Thus $aba^{-1}b^{-1} = e \implies ab = ba$. So G is abelian. By the Fundamental Theorem of Finite Abelian Groups

$$G \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq},$$

which is cyclic. □

Example 4.1.3

By the Fundamental Theorem of Finite Abelian Groups

$$S_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3,$$

and $|S_3| = 6 = 2 \cdot 3$, is not cyclic.

Example 4.1.4

If $|G| = 30$, then G has a subgroup isomorphic to $\mathbb{Z}_{15}$. Note that $|G| = 2 \cdot 3 \cdot 5$. By the Third Sylow Theorem,

$$n_5 \equiv 1 \mod 5 \text{ and } n_5 \mid 6 \implies n_5 = 1 \text{ or } 6$$

and

$$n_3 \equiv 1 \mod 3 \text{ and } n_3 \mid 10 \implies n_3 = 1 \text{ or } 10.$$

Suppose $n_5 = 6$ and $n_3 = 10$. Since the Sylow 3-subgroups and Sylow 5-subgroups intersect trivially, this accounts for $(6 \times 4) + (10 \times 2) = 44$ elements but $|G| = 30 < 44$. Thus we must have $n_5 = 1$ or $n_3 = 1$. Thus G is not simple.

Let H_3 and H_5 be Sylow 3- and 5-subgroups, respectively. WLOG, suppose $H_3 \triangleleft G$. Then $H_3H_5 \leq G$, and notice that $|H_3H_5| = 15$. Since $15 = 3 \cdot 5$ and $3 \nmid 4 = 5 - 1$, we know that $H_3H_5 \simeq \mathbb{Z}_{15}$ by an earlier example.

Example 4.1.5

Let $|G| = 60$ with $n_5 > 1$. Then G is simple.

This is an important example for it is with this that we can prove the following:

Corollary 12 (A_5 is Simple)

A_5 is simple.

Proof

Note that $|A_5| = \frac{5!}{2} = 60$, and

$$\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\rangle \text{ and } \left\langle \begin{pmatrix} 1 & 3 & 2 & 4 & 5 \end{pmatrix} \right\rangle$$

are both Sylow 5-subgroups that are distinct (one has odd **parity** while the other has even).

Proof (For Example 4.1.5)

Suppose $n_5 > 1$. Notice that $60 = 2^2 \cdot 3 \cdot 5$. By Theorem 11, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 12$, and thus $n_5 = 6$. This accounts for $6 \times 4 + 1 = 25$ elements. Now suppose $H \triangleleft G$ is proper and non-trivial.

If $5 \mid |H|$, then H contains a Sylow 5-subgroup of G. Since $H \triangleleft G$, H contains all the conjugates of this Sylow 5-subgroup. Thus by our argument above, we have that $|H| \geq 25$ [2]. Also, $H \mid 60$. Thus it must be that $|H| = 30$. But then by the last example, $n_5 = 1$, a contradiction.

So $5 \nmid |H|$. By Lagrange, it remains that

$$|H| = 2,\ 3,\ 4,\ 6 \text{ or } 12.$$

Case A $|H| = 12 = 2^2 \cdot 3$.[3] So H contains a normal Sylow 2- or

[2] These are the 25 elements that were found in the last paragraph.

[3]

Exercise 4.1.1
Prove that either $n_2 = 1$ or $n_3 = 1$.

3-subgroup that is normal in G.

The proof shall be continued next lecture.

Part II

Fields

5 Lecture 5 Jan 14th

5.1 Sylow Theory (Continued 3)

We shall continue with the last proof from where we left off.

Proof (Example 4.1.5 continued)

Case A $|H| = 12$. WLOG, let K be a normal Sylow 3-subgroup of H, which is also normal in G [1].

Case B $|H| = 6$. H would then have a normal Sylow 3-subgroup, which is normal in G. We shall also call this subgroup K.

By replacing H with K if necessary, wma $|H| \in \{2,3,4\}$. Consider $\overline{G} = G/H$. Then $\left|\overline{G}\right| \in \{15,20,30\}$. [2] In any case, $\overline{G}$ has a normal Sylow 5-subgroup. Call this normal subgroup $\overline{P}$. By correspondence, $\overline{P} = P/H$ where P is a normal subgroup of G [3]. Thus P is a proper non-trivial normal subgroup of G. Also,

$$|P| = \left|\overline{P}\right| \cdot |H| = 5 \cdot |H|.$$

Thus $5 \mid |P|$, putting us back to the case where $5 \mid |H|$. Thus G does not have a non-trivial normal subgroup, i.e. G is simple. □

[1] In Sylow Theory, normality is transitive.

[2]

Exercise 5.1.1
Prove that $\overline{G}$ has a normal Sylow 5-subgroup in all the three possible orders of $\overline{G}$.

[3] Note: correspondence works for the normal case as well.

5.2 Review of Ring Theory

Let F be a **field**, and I be an **ideal** of $F[x]$, its **polynomial ring**. Since $F[x]$ is a PID, we have $I = \langle p(x) \rangle$ for some $p(x) \in F[x]$.

Moreover, I is **maximal** iff $p(x)$ is **irreducible**.

Thus we observe that

$F[x]/I$ is a field iff $I = \langle p(x) \rangle$ is maximal iff $p(x) \in F[x]$ is irreducible.

Therefore, to talk about fields, we need to understand irreducibles.

5.3 Irreducibles

Definition 6 (Irreducible)

Let R be an integral domain (ID) [4]*. We say that $f(x) \in R[x]$ is **irreducible** (over R) if*

1. $f(x) \neq 0$;
2. $f(x) \notin R^\times$, *where $R^\times$ is the set of units of R;*
3. *whenever $f(x) = g(x)h(x)$, where $g(x), h(x) \in R[x]$, then either $g(x) \in R^\times$ or $h(x) \in R^\times$.*

*If $f(x) \neq 0$, $f(x) \notin R^\times$ and $f(x)$ is not irreducible, we say that $f(x)$ is **reducible** (over R).*

[4] **Integral domains** are commutative rings that has no zero divisors.

Example 5.3.1

$f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$ as

$$f(x) = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right).$$

Let F be a field, $f(x) \in F[x]$ and $a \in F$. By the **Division Algorithm**, we can write

$$f(x) = (x - a)q(x) + r(x),$$

where $q(x), r(x) \in F[x]$. Note that we either have $r(x) = 0$ or $\deg r < \deg(x - a) = 1$. In the latter case, $r \in F$, and so

$$f(x) = (x - a)q(x) + r.$$

Then $f(a) = 0 + r = r$, and so $f(x) = (x - a)q(x) + f(a)$.

$$\therefore (x - a) \mid f(x) \iff f(a) = 0.$$

Proposition 13 (Polynomials with Roots are Reducible)

Let F be a field. If $f(x) \in F[x]$ with $\deg f > 1$, and f has a root in F, then f is reducible (over F).

Example 5.3.2

Let $f(x) = x^6 + x^3 + x^4 + x^3 + 3 \in \mathbb{Z}_7[x]$. Then $f(1) = 0$. Therefore

$$f(x) = (x-1)g(x) \text{ where } g(x) \in \mathbb{Z}_7[x].$$

Thus $f(x)$ is reducible over $\mathbb{Z}_7$.

Proposition 14 (Irreducible Rootless Polynomials)

Let F be a field[5]*. If $f(x) \in F[x]$ with $\deg f \in \{2,3\}$, then $f(x)$ is irreducible over F iff $f(x)$ has no roots in F.*

[5] Note that this does not work in an ID. For example, $2x^2 + 2$.

Warning

$(x^2+1)^2 \in \mathbb{R}[x]$ is reducible but has no root in $\mathbb{R}$. Note that the degree of the polynomial is 4.

Example 5.3.3

Let $f9x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Note that $f(0) = 1$ and $f(1) = 3 \equiv 1 \mod 2$. Since $\deg f = 3$ and f has no roots in $\mathbb{Z}_2$, $f(x)$ is irreducible over $\mathbb{Z}_2$.

Theorem 15 (Gauss' Lemma)

Let R be a Unique Factorization Domain (UFD), with field of fractions F. Let $p(x) \in R[x]$. If

$$p(x) = A(x)B(x),$$

where $A(x), B(x)$ are non-constant in $F[x]$, then $\exists r, s \in F^\times$ non-zero such that

$$p(x) = a(x)b(x),$$

where $a(x) = rA(x)$ and $b(x) = sB(x)$.

Note

If $p(x) \in R[x]$ is reducible over F, then $p(x)$ is reducible over R.

Note

If $R = \mathbb{Z}$ and $F = \mathbb{Q}$, then $p(x)$ is irreducible over $\mathbb{Z}$, then $p(x)$ is irreducible over $\mathbb{Q}$.

6 Lecture 6 Jan 18th

6.1 Irreducibles (Continued)

Our goal in this section is to develop methods to test for the irreducibility of polynomials.

Warning

Note that $f(x) = 2x+4 = 2(x+2)$ *is reducible ovver* $\mathbb{Z}$ [1] *but irreducible over* $\mathbb{Q}$.

[1] This is interesting over $\mathbb{Z}$, since $2 \notin \mathbb{Z}^\times$.

Proposition 16 (Mod-p Irreducibility Test)

Let $f(x) \in \mathbb{Z}[x]$ *with* $\deg f \geq 1$. *Let* $p \in \mathbb{Z}$ *be prime. If* $\bar{f}(x)$ *is the corresponding polynomial in* $\mathbb{Z}_p[x]$ *such that*

- *the coefficients of* $\bar{f}(x)$ *are coefficients of* $f(x)$ *in mod* p,
- $\deg f = \deg \bar{f}$ [2], *and*
- $\bar{f}$ *is irreducible over* $\mathbb{Z}_p$,

then $f(x)$ *is irreducible over* $\mathbb{Q}$.

[2] This means that the leading coefficient of f is not killed off.

Proof

Suppose $\deg f = \deg \bar{f}$, and $\bar{f}(x) \in \mathbb{Z}_p$ is irreducible over $\mathbb{Z}_p$. Suppose to the contrary that $f(x)$ is reducible over $\mathbb{Q}$. Then for some $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg g, \deg h < \deg f$, we have

$$f(x) = g(x)h(x).$$

By Gauss' Lemma, wma $g(x), h(x) \in \mathbb{Z}[x]$. Then we have

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x) \in \mathbb{Z}_p[x].$$

By assumption, $\bar{f}$ is irreducible over $\mathbb{Z}_p$, either

$$\deg \bar{g} = 0 \text{ or } \deg \bar{h} = 0.$$

Wlog, $\deg \bar{g} = 0$. Then

$$\deg h \leq \deg f = \deg \bar{f} = \deg \bar{h} \leq \deg h,$$

which implies that $\deg f = \deg h$ but $\deg h < \deg f$. Thus f is irreducible over $\mathbb{Q}$. □

Example 6.1.1

Consider the polynomial

$$f(x) = 3x^3 + 22x^2 + 17x + 471.$$

Then consider

$$\bar{f}(x) = x^3 + x + 1 \in \mathbb{Z}_2[x].$$

Since $\bar{f}(0) \neq 0$ and $\bar{f}(1) \neq 0$, and $\deg f = 3$, by Proposition 14, $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2$. Since $\deg f = \deg \bar{f}$, f is irreducible over $\mathbb{Q}$ by the Mod-2 irreducible test.

Warning

*Consider $f(x) = 2x^2 + x \in \mathbb{Q}[x]$, which is reducible over $\mathbb{Q}$. However, $\bar{f}(x) = x \in \mathbb{Z}_2[x]$ is **reducible** over $\mathbb{Z}_2$. Notice here that $\deg \bar{f} \neq \deg f$.*

More generally so...

Proposition 17 (Polynomials that Cannot be Factored Over the Ideals is Irreducible)

Let I be a proper ideal of an ID R. Let $p(x) \in R[x]$ be monic and non-const. If $p(x)$ cannot be factored in $(R/I)[x]$ [3] into polynomials of lesser degree, then $p(x)$ is irreducible over R.

[3] Note that (R/I) may not be an ID even if R is one.

Proof

Sps to the contrary that $p(x)$ is reducible over R. Then

$$p(x) = f(x)g(x)$$

for some $f(x), g(x) \notin R^\times$. Since $p(x)$ is monic, and $\deg f, \deg g < \deg p$, wma $f(x)$ and $g(x)$ are also monic. Then

$$\overline{p}(x) = \overline{f}(x)\overline{g}(x) \in (R/I)[x].$$

Since $I \subsetneq R$, we have that $1 \notin I$, and so

$$\deg \overline{f}, \deg \overline{g} < \deg \overline{p}$$

but that implies that $p(x)$ can be factored in $(R/I)[x]$. □

Proposition 18 (Eisenstein's Criterion)

Let R be an ID. Let P be a prime ideal of R. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$$

with $n \geq 1$. Note that f is monic. Now if

$$a_{n-1}, a_{n-2}, \ldots, a_1, a_0 \in P \text{ and } a_0 \notin P^2,$$

then f is irreducible over R.

Proof

Sps to the contrary that f is reducible over R. Since $f(x)$ is monic,

$$f(x) = g(x)h(x)$$

where $g(x), h(x) \in R[x]$ and $\deg g, \deg h < \deg f$. Then

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x) = x^n \in (R/P)[x]$$

since $a_{n-1}, a_{n-2}, \ldots, a_1, a_0 \in P$. Since P is prime, R/P is an ID, we have that either $\overline{g}(0) = 0$ or $\overline{h}(0) = 0$. Wlog, $\overline{g}(0) = 0 \in P$. But that

implies that $a_0 = \bar{g}(0)\bar{h}(0) = 0 \in P^2$, a contradiction. □

A Asides and Prior Knowledge

A.1 Correspondence Theorem

The Correspondence Theorem is somewhat widely known as the Fourth Isomorphism Theorem, although some authors associates the name with a proposition known as Zaessenhaus Lemma.

Theorem A.1 (Correspondence Theorem)

Let G be a group, and $N \triangleleft G$ [1]. Then there exists a bijection between the set of all subgroups $A \leq G$ such that $A \supseteq N$ and the set of subgroups A/N of G/N.

[1] Recall that this symbol means that N is a normal subgroup of G.

Proof

Index