# Algebra Notes

D. Zack Garza

January 6, 2020

## Contents

**1 Group Theory** **1**
- 1.1 Finitely Generated Abelian Groups . . . 2
- 1.2 The Symmetric Group . . . 3
- 1.3 Counting Theorems . . . 4
  - 1.3.1 Examples of Orbit-Stabilizer . . . 5
  - 1.3.2 Sylow Theorems . . . 5
  - 1.3.3 Sylow 1 (Cauchy for Prime Powers) . . . 6
  - 1.3.4 Sylow 2 (Sylows are Conjugate) . . . 6
  - 1.3.5 Sylow 3 (Numerical Constraints) . . . 6
- 1.4 Products . . . 6
- 1.5 Isomorphism Theorems . . . 7
- 1.6 Special Classes of Groups . . . 8
- 1.7 Series of Groups . . . 9

**2 Rings** **10**
- 2.1 Definitions and Basics . . . 10
- 2.2 Maximal and Prime Ideals . . . 10
- 2.3 Nilradical and Jacobson Radical . . . 11
- 2.4 Zorn's Lemma . . . 11
- 2.5 Unsorted . . . 12

**3 Fields** **12**
- 3.1 Cyclotomic Polynomials . . . 12
- 3.2 Finite Fields . . . 13
- 3.3 Galois Theory . . . 14

# 1 Group Theory

**Definition (Centralizer)**:

$$C_G(H) = \left\{ g \in G \;\middle|\; ghg^{-1} = h \;\forall h \in H \right\}$$

**Definition (Normalizer)**:

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

**Lemma:** $C_G(H) \leq N_G(H)$

**Lemma:** The size of the conjugacy class of $H$ is the index of the centralizer, i.e.

$$\left| \left\{ gHg^{-1} \;\middle|\; g \in G \right\} \right| = [G : C_G(H)].$$

**Lemma ("The Fundamental Theorem of Cosets")**:

$$aH = bH \iff a^{-1}b \in H \text{ or } aH \bigcap bH = \emptyset$$

Definition: $[x, y] = x^{-1}y^{-1}xy$ is the **commutator**, and $[G, G] \coloneqq \left\{ [x, y] \;\middle|\; x, y \in G \right\}$ is the **commutator subgroup**.

**Lemma:**

$$[G, G] \leq H \text{ and } H \trianglelefteq G \implies G/H \text{ is abelian.}$$

## 1.1 Finitely Generated Abelian Groups

Invariant factor decomposition:

$$G \cong \mathbb{Z}^r \times \prod_{j=1}^{m} \mathbb{Z}/(n_j) \quad \text{where } n_1 \;\middle|\; \cdots \;\middle|\; n_m.$$

**Going from invariant divisors to elementary divisors:**

- Take prime factorization of each factor
- Split into coprime pieces

*Example:*

$$\begin{aligned} &\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3 \cdot 5^2 \cdot 7) \\ \cong &\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2^3) \oplus \mathbb{Z}/(5^2) \oplus \mathbb{Z}/(7) \\ &. \end{aligned}$$

**Going from elementary divisors to invariant factors:**

- Bin up by primes occurring (keeping exponents)
- Take highest power from each prime as *last* invariant factor
- Take highest power from all remaining primes as next, etc

*Example:* Given the invariant factor decomposition

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}, .$$

| $p=2$ | $p=3$ | $p=5$ |
|---|---|---|
| $2,2,2$ | $3,3$ | $5^2$ |

$\implies n_m = 5^2 \cdot 3 \cdot 2$

| $p=2$ | $p=3$ | $p=5$ |
|---|---|---|
| $2,2$ | $3$ | $\emptyset$ |

$\implies n_{m-1} = 3 \cdot 2$

| $p=2$ | $p=3$ | $p=5$ |
|---|---|---|
| $2$ | $\emptyset$ | $\emptyset$ |

$\implies n_{m-2} = 2$

and thus

$$G \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(3 \cdot 2) \oplus \mathbb{Z}/(5^2 \cdot 3 \cdot 2).$$

## 1.2 The Symmetric Group

**Definitions:**

- A cycle is **even** $\iff$ product of an *even* number of transpositions.
  - A cycle of even *length* is **odd**
  - A cycle of odd *length* is **even**

**Definition** The **alternating group** is the subgroup of **even** permutations, i.e. $A_n \coloneqq \left\{\sigma \in S_n \;\middle|\; \operatorname{sign}(\sigma) = 1\right\}$ where $\operatorname{sign}(\sigma) = (-1)^m$ where $m$ is the number of cycles of even length.

*Corollary:* Every $\sigma \in A_n$ has an even number of *odd* cycles (i.e. an even number of *even-length* cycles).

*Example:*

$$\begin{aligned} A_4 = \{&\mathrm{id}, \\ &(1,3)(2,4), (1,2)(3,4), (1,4)(2,3), \\ &(1,2,3), (1,3,2), \\ &(1,2,4), (1,4,2), \\ &(1,3,4), (1,4,3), \\ &(2,3,4), (2,4,3)\}. \end{aligned}$$

**Lemmas:**

- The transitive subgroups of $S_3$ are $S_3, A_3$

- The transitive subgroups of $S_4$ are $S_4, A_4, D_4, \mathbb{Z}_2^2, \mathbb{Z}_4$.
- For $n = 4, S_n$ has two normal subgroups: $A_4, \mathbb{Z}_2^2$.
- For $n \geq 5, S_n$ one normal subgroup: $A_n$.
- $Z(S_n) = 1$ for $n \geq 3$
- $Z(A_n) = 1$ for $n \geq 4$
- $[S_n, S_n] = A_n$
- $[A_4, A_4] \cong \mathbb{Z}_2^2$
- $[A_n, A_n] = A_n$ for $n \geq 5$
- $A_n$ is *simple* for $n \geq 5$.

## 1.3 Counting Theorems

**Lagrange's Theorem**:

$$H \leq G \implies |H| \,\Big|\, |G|.$$

*Corollary*: The order of every element divides the size of $G$, i.e.

$$g \in G \implies o(g) \,\Big|\, o(G) \implies g^{|G|} = e.$$

> **Warning:** Rhere does **not** necessarily exist $H \leq G$ with $|H| = n$ for every $n \,\Big|\, |G|$.
> Counterexample: $|A_4| = 12$ but has no subgroup of order 6.

**Cauchy's Theorem**:

For every prime $p$ dividing $|G|$. there is an element (and thus a subgroup) of order $p$.

> This is a partial converse to Lagrange's theorem.

**Notation:** For a group $G$ acting on a set $X$,

- $G \cdot x = \left\{ g \curvearrowright x \;\middle|\; g \in G \right\} \subseteq X$ is the orbit
- $G_x = \left\{ g \in G \;\middle|\; g \curvearrowright x = x \right\} \subseteq G$ is the stabilizer
- $X/G \subset \mathcal{P}(X)$ is the set of orbits
- $X^g = \left\{ x \in X \;\middle|\; g \curvearrowright x = x \right\} \subseteq X$ are the fixed points

**Orbit-Stabilizer**:

$$|G \cdot x| = [G : G_x] = |G|/|G_x| \quad \text{if } G \text{ is finite}$$

> Mnemonic: $G/G_x \cong G \cdot x$.

### 1.3.1 Examples of Orbit-Stabilizer

1. Let $G$ act on itself by conjugation.

- $G \cdot x$ is the **conjugacy class** of $x$
- $G_x = Z(x) \coloneqq C_G(x) = \left\{ g \;\middle|\; [g, x] = e \right\}$, the **centralizer** of $x$.
- $G^g$ (the fixed points) is the **center** $Z(G)$.

> *Corollary:* The size of a conjugacy class is the index of the centralizer.
> *Corollary*: the **Class Equation**:
>
> $$|G| = |Z(G)| + \sum_{\substack{\text{One } x_i \text{ from} \\ \text{each conjugacy} \\ \text{class}}} [G : Z(x_i)]$$

1. Let $G$ act on $S$, its set of *subgroups*, by conjugation.

- $G \cdot H = \left\{ gHg^{-1} \right\}$ is the **set of conjugate subgroups** of $H$
- $G_H = N_G(H)$ is the **normalizer** of in $G$ of $H$
- $S^G$ is the set of **normal subgroups** of $G$

3. For a fixed proper subgroup $H < G$, let $G$ act on its cosets $G/H = \left\{ gH \;\middle|\; g \in G \right\}$ by left-multiplication.

- $G \cdot gH = G/H$, i.e. this is a *transitive* action.
- $G_{gH} = gHg^{-1}$ is a *conjugate subgroup* of $H$
- $(G/H)^G = \emptyset$

> *Application:* If $G$ is simple, $H < G$ proper, and $[G : H] = n$, then there exists an injective map $\phi : G \hookrightarrow S_n$.
> *Proof:* This action induces $\phi$; it is nontrivial since $gH = H$ for all $g$ implies $H = G$; $\ker \phi \trianglelefteq G$ and $G$ simple implies $\ker \phi = 1$.

**Burnside's Formula:**

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

### 1.3.2 Sylow Theorems

**Notation**: For any $p$, let $\mathrm{Syl}_p(G)$ be the set of Sylow-$p$ subgroups of $G$.

Write

- $|G| = p^n m$ where $(m, p) = 1$,
- $S_p$ a Sylow-$p$ subgroup, and
- $n_p$ the number of Sylow-$p$ subgroups.

**Definition**: A $p$-group is a group $G$ such that every element is order $p^k$ for some $k$. If $G$ is a finite $p$-group, then $|G| = p^j$ for some $j$.

**Lemma:** $p$-groups have nontrivial centers.

Some useful facts:

- Coprime order subgroups are disjoint, or more generally $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \bigcap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$.
- The Chinese Remainder theorem: $(p,q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

### 1.3.3 Sylow 1 (Cauchy for Prime Powers)

$$\forall p^n \text{ dividing } |G| \quad \text{there exists a subgroup of size } p^n.$$

If $|G| = \prod p_i^{\alpha_i}$, then there exist subgroups of order $p_i^{\beta_i}$ for every $i$ and every $0 \leq \beta_i \leq \alpha_i$. In particular, Sylow $p$-subgroups always exist.

### 1.3.4 Sylow 2 (Sylows are Conjugate)

All sylow-$p$ subgroups $S_p$ are conjugate, i.e.

$$S_p^1, S_p^2 \in \mathrm{Syl}_p(G) \implies \exists g \text{ such that } gS_p^1 g^{-1} = S_p^2.$$

**Corollary**: $n_p = 1 \iff S_p \trianglelefteq G$

### 1.3.5 Sylow 3 (Numerical Constraints)

1. $n_p \Big| m$ (in particular, $n_p \leq m$),
2. $n_p \equiv 1 \mod p$,
3. $n_p = [G : N_G(S_p)]$ where $N_G$ is the normalizer.

**Corollary:** $p$ does not divide $n_p$.

**Lemma:** Every $p$-subgroup of $G$ is contained in a Sylow $p$-subgroup.

*Proof:* Let $H \leq G$ be a $p$-subgroup. If $H$ is not *properly* contained in any other $p$-subgroup, it is a Sylow $p$-subgroup by definition.
Otherwise, it is contained in some $p$-subgroup $H^1$. Inductively this yields a chain $H \subsetneq H^1 \subsetneq \cdots$, and by Zorn's lemma $H := \bigcup_i H^i$ is maximal and thus a Sylow $p$-subgroup.

**Fratini's Argument**: If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(G)$, then $HN_G(P) = G$ and $[G : H]$ divides $|N_G(P)|$.

## 1.4 Products

**Characterizing direct products**: $G \cong H \times K$ when

- $G = HK = \left\{ hk \;\middle|\; h \in H, k \in K \right\}$
- $H \bigcap K = \{e\} \subset G$

- $H, K \trianglelefteq G$

Can relax to only $H \trianglelefteq G$ to get a semidirect product instead

**Characterizing semidirect products**: $G = N \rtimes_\psi H$ when

- $G = NH$
- $N \trianglelefteq G$
- $H \curvearrowright N$ by conjugation via a map

$$\begin{aligned} \psi : H &\to \mathrm{Aut}(N) \\ h &\mapsto h(\,\cdot\,)h^{-1}. \end{aligned}$$

*Lemma:* If $\sigma \in \mathrm{Aut}(H)$, then $N \rtimes_\psi H \cong N \rtimes_{\psi\circ\sigma} H$.

**Useful Facts**

- $\mathrm{Aut}(\prod_{k=1}^{n} \mathbb{Z}/(p)) = \mathrm{GL}(n, \mathbb{Z}/(p))$
  - If this occurs in a semidirect product, it suffices to consider similarity classes of matrices (i.e. just use canonical forms)
- $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}^n)^\times \cong \mathbb{Z}^{\varphi(n)}$ where $\varphi$ is the totient function.

## 1.5 Isomorphism Theorems

**Lemma:** If $H, K \leq G$ and $H \leq N_G(K)$ (or $K \trianglelefteq G$) then $HK \leq G$ is a subgroup.

**Diamond Theorem / 2nd Isomorphism Theorem**:

If $S \leq G$ and $N \trianglelefteq G$, then

$$\frac{SN}{N} \cong \frac{S}{S \bigcap N}$$

Note: for this to make sense, we also have

- $SN \leq G$,
- $S \bigcap N \trianglelefteq S$,

**Cancellation / 3rd Isomorphism Theorem**

If $H, K \trianglelefteq G$ with $H \trianglelefteq K$, then

$$\frac{G/H}{G/K} \cong \frac{G}{K}$$

Note: for this to make sense, we also have $G/K \trianglelefteq G/H$.

**The Correspondence Theorem / 4th Isomorphism Theorem:** Suppose $N \trianglelefteq G$, then there exists a correspondence:

Figure 1: Image

$$\left\{H < G \;\middle|\; N \subseteq H\right\} \iff \left\{H \;\middle|\; H < \frac{G}{N}\right\}$$
$$\{\} \iff \{\}\,.$$

In words, subgroups of $G$ containing $N$ correspond to subgroups of the quotient group $G/N$. This is given by the map $H \mapsto H/N$.

Note: $N \trianglelefteq G$ and $N \subseteq H < G \implies N \trianglelefteq H$.

## 1.6 Special Classes of Groups

**Definition:** The **"2 out of 3 property"** is satisfied by a class of groups $\mathcal{C}$ iff whenever $G \in \mathcal{C}$, then $N, G/N \in \mathcal{C}$ for any $N \trianglelefteq G$.

**Definition:** If $|G| = p^k$, then $G$ is a **p-group.**

**Lemmas:**

- p-groups have nontrivial centers
- Every normal subgroup is contained in the center
- Normalizers grow
- Every maximal is normal
- Every maximal has index $p$
- p-groups are *nilpotent*
- p-groups are *solvable*

**Definition:** A group $G$ is **simple** iff $H \trianglelefteq G \implies H = \{e\}, G$, i.e. it has no non-trivial proper subgroups.

**Lemma:** If $G$ is *not* simple, then for any $N \trianglelefteq G$, it is the case that $G \cong E$ for an extension of the form $N \to E \to G/N$. >

**Definition:** A group $G$ is **solvable** iff $G$ has a terminating normal series with abelian factors, i.e.

$$G \to G^1 \to \cdots \to \{e\} \text{ with } G^i/G^{i+1} \text{ abelian for all } i.$$

**Lemmas:**

- $G$ is solvable iff $G$ has a terminating *derived series*.
- Solvable groups satisfy the 2 out of 3 property
- Abelian $\implies$ solvable
- Every group of order less than 60 is solvable.

**Definition:** A group $G$ is **nilpotent** iff $G$ has a terminating central series, upper central series, or lower central series.

Moral: the adjoint map is nilpotent.

**Lemma:** For $G$ a finite group, TFAE:

- $G$ is nilpotent
- Normalizers grow (i.e.$H < N_G(H)$ whenever $H$ is proper)
- Every Sylow-p subgroup is normal
- $G$ is the direct product of its Sylow p-subgroups
- Every maximal subgroup is normal
- $G$ has a terminating *Lower* Central Series
- $G$ has a terminating *Upper* Central Series

**Lemmas:**

- $G$ nilpotent $\implies$ $G$ solvable
- Nilpotent groups satisfy the 2 out of 3 property.
- $G$ has normal subgroups of order $d$ for *every* $d$ dividing $|G|$
- $G$ nilpotent $\implies$ $Z(G) \neq 0$
- Abelian $\implies$ nilpotent
- p-groups $\implies$ nilpotent

## 1.7 Series of Groups

**Definition**: A **normal series** of a group $G$ is a sequence $G \to G^1 \to G^2 \to \cdots$ such that $G^{i+1} \trianglelefteq G_i$ for every $i$.

**Definition** A **composition series** of a group $G$ is a finite normal series such that $G^{i+1}$ is a *maximal proper* normal subgroup of $G^i$.

**Theorem (Jordan-Holder)**: Any two composition series of a group have the same length and isomorphic factors (up to permutation).1

**Definition** A **derived series** of a group $G$ is a normal series $G \to G^1 \to G^2 \to \cdots$ where $G^{i+1} = [G^i, G^i]$ is the commutator subgroup.

The derived series terminates iff $G$ is *solvable*.

**Definition:** A **central series** for a group $G$ is a terminating normal series $G \to G^1 \to \cdots \to \{e\}$ such that each quotient is **central**, i.e. $[G, G^i] \leq G^{i-1}$ for all $i$.

**Definition:** A **lower central series** is a terminating normal series $G \to G^1 \to \cdots \to \{e\}$ such that $G^{i+1} = [G^i, G]$

Moral: Iterate the adjoint map $[\cdot, G]$.

$G$ is nilpotent $\iff$ the LCS terminates.

**Definition:** An **upper central series** is a terminating normal series $G \to G^1 \to \cdots \to \{e\}$ such that $G^1 = Z(G)$ and $G^{i+1}$ is defined such that $G^{i+1}/G^i = Z(G^i)$.

Moral: Iterate taking "higher centers".

# 2 Rings

## 2.1 Definitions and Basics

**Definition:** $\mathfrak{p}$ is a **prime** ideal $\iff ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

**Definition:** $\operatorname{Spec}(R) = \left\{ \mathfrak{p} \trianglelefteq R \;\middle|\; \mathfrak{p} \text{ is prime} \right\}$ is the **spectrum** of $R$.

**Definition:** $\mathfrak{m}$ is **maximal** $\iff I \trianglelefteq R \implies I \subseteq \mathfrak{m}$.

**Definition:** $\operatorname{Spec}_{\max}(R) = \left\{ \mathfrak{m} \trianglelefteq R \;\middle|\; \mathfrak{m} \text{ is maximal} \right\}$ is the **max-spectrum** of $R$.

Note: nonstandard notation / definition.

**Lemma:** Field $\implies$ Euclidean Domain $\implies$ PID $\implies$ UFD $\implies$ Integral Domain.

## 2.2 Maximal and Prime Ideals

**Lemma:** Maximal $\implies$ prime, but generally not the converse.

*Counterexample*: $(0) \in \mathbb{Z}$ is prime since $\mathbb{Z}$ is a domain, but not maximal since it is properly contained in any other ideal.

*Proof:* Suppose $\mathfrak{m}$ is maximal, $ab \in \mathfrak{m}$, and $b \notin \mathfrak{m}$. Then there is a containment of ideals $\mathfrak{m} \subsetneq \mathfrak{m} + (b) \implies \mathfrak{m} + (b) = R$.
So

$$1 = m + rb \implies a = am + r(ab),$$

but $am \in \mathfrak{m}$ and $ab \in \mathfrak{m} \implies a \in \mathfrak{m}$.

■

**Lemma:** If $x$ is not a unit, then $x$ is contained in some maximal ideal $\mathfrak{m}$.

*Proof:* Zorn's lemma.

**Lemma:** $R/\mathfrak{m}$ is a field $\iff \mathfrak{m}$ is maximal.

**Lemma:** $R/\mathfrak{p}$ is an integral domain $\iff \mathfrak{p}$ is prime.

## 2.3 Nilradical and Jacobson Radical

**Definition:** $\mathfrak{N} \coloneqq \left\{ x \in R \;\middle|\; x^n = 0 \text{ for some } n \right\}$ is the **nilradical** of $R$.

**Lemma:** The nilradical is the intersection of all **prime** ideals, i.e.

$$\mathfrak{N}(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$$

*Proof:*
$\mathfrak{N} \subseteq \bigcap \mathfrak{p}$: $x \in \mathfrak{N} \implies x^n = 0 \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $x^{n-1} \in \mathfrak{p}$.
$\mathfrak{N}^c \subseteq \bigcup \mathfrak{p}^c$: Define $S = \left\{ I \trianglelefteq R \;\middle|\; a^n \notin I \text{ for any } n \right\}$. Then apply Zorn's lemma to get a maximal ideal $\mathfrak{m}$, and maximal $\implies$ prime.

**Lemma:** $R/\mathfrak{N}(R)$ has no nonzero nilpotent elements.

*Proof:*

$$\begin{aligned} a + \mathfrak{N}(R) \text{ nilpotent} &\implies (a + \mathfrak{N}(R))^n \coloneqq a^n + \mathfrak{N}(R) = \mathfrak{N}(R) \\ &\implies a^n \in \mathfrak{N}(R) \\ &\implies \exists \ell \text{ such that } (a^n)^\ell = 0 \\ &\implies a \in \mathfrak{N}(R). \end{aligned}$$

**Definition:** The **Jacobson radical** is the intersection of all **maximal** ideals, i.e.

$$J(R) = \bigcap_{\mathfrak{m} \in \operatorname{Spec}_{\max}} \mathfrak{m}$$

**Lemma:** $\mathfrak{N}(R) \subseteq J(R)$.

*Proof:* Maximal $\implies$ prime, and so if $x$ is in every prime ideal, it is necessarily in every maximal ideal as well.

## 2.4 Zorn's Lemma

**Lemma**: A field has no nontrivial proper ideals.

**Lemma:** If $I \trianglelefteq R$ is a proper ideal $\iff$ $I$ contains no units.

*Proof:* $r \in R^\times \bigcap I \implies r^{-1} r \in I \implies 1 \in I \implies x \cdot 1 \in I \quad \forall x \in R.$

**Lemma:** If $I_1 \subseteq I_2 \subseteq \cdots$ are ideals then $\bigcup_j I_j$ is an ideal.

**Example Application of Zorn's Lemma:** Every proper ideal is contained in a maximal ideal.

*Proof:* Let $0 < I < R$ be a proper ideal, and consider the set

$$S = \left\{ J \;\middle|\; I \subseteq J < R \right\}.$$

Note $I \in S$, so $S$ is nonempty. The claim is that $S$ contains a maximal element $M$.
$S$ is a poset, ordered by set inclusion, so if we can show that every chain has an upper bound, we can apply Zorn's lemma to produce $M$.
Let $C \subseteq S$ be a chain in $S$, so $C = \{C_1 \subseteq C_2 \subseteq \cdots\}$ and define $\hat{C} = \bigcup_i C_i$.

**$\hat{C}$ is an upper bound for $C$:**
This follows because every $C_i \subseteq \hat{C}$.
**$\hat{C}$ is in $S$:**
Use the fact that $I \subseteq C_i < R$ for every $C_i$ and since no $C_i$ contains a unit, $\hat{C}$ doesn't contain a unit, and is thus proper.

■

### 2.5 Unsorted

**Lemma:** Every $a \in R$ for a finite ring is either a unit or a zero divisor.

*Proof:* Let $a \in R$ and define $\phi(x) = ax$. If $\phi$ is injective, then it is surjective, so $1 = ax$ for some $x \implies x^{-1} = a$. Otherwise, $ax_1 = ax_2$ with $x_1 \neq x_2 \implies a(x_1 - x_2) = 0$ and $x_1 - x_2 \neq 0$, so $a$ is a zero divisor.

## 3 Fields

**Lemma:** Let $\phi_n \coloneqq x^{p^n} - x$. Then $f(x) \;\middle|\; \phi_n(x) \iff \deg f \;\middle|\; n$ and $f$ is irreducible.

(So $\phi_n = \prod f_i(x)$ over all irreducible monic $f_i$ of degree $d$ dividing $n$.)

*Proof:*
$\impliedby$:
Suppose $f$ is irreducible of degree $d$. Then $f \;\middle|\; x^{p^d} - x$ (consider $F[x]/\langle f \rangle$) and $x^{p^d} - x \;\middle|\; x^{p^n} - x \iff d \;\middle|\; n$.
$\implies$:

- $\alpha \in \mathbb{GF}(p^n) \iff \alpha^{p^n} - \alpha = 0$, so every element is a root of $\phi_n$ and $\deg \min(\alpha, \mathbb{F}_p) \;\middle|\; n$ since $\mathbb{F}_p(\alpha)$ is an intermediate extension.
- So if $f$ is an irreducible factor of $\phi_n$, $f$ is the minimal polynomial of some root $\alpha$ of $\phi_n$, so $\deg f \;\middle|\; n$. $\phi_n'(x) = p^n x^{p^n - 1} \neq 0$, so $\phi_n$ has distinct roots and thus no repeated factors. So $\phi_n$ is the product of all such irreducible $f$.

### 3.1 Cyclotomic Polynomials

**Definition:** Let $\zeta_n = e^{2\pi i/n}$, then

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (j,n)=1}}^{n} \left( x - \zeta_n^k \right)$$

**Corollary:** $\deg \Phi_n(x) = \phi(n)$ for $\phi$ the totient function.

**Computing $\Phi_n$:**

1.
$$\Phi_n(z) = \prod_{d|n, d>0} \left(z^d - 1\right)^{\mu\left(\frac{n}{d}\right)}$$

where

$$\mu(n) \equiv \begin{cases} 0 & \text{if } n \text{ has one or more repeated prime factors} \\ 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes,} \end{cases}$$

2.
$$x^n - 1 = \prod_{d|n} \Phi_d(x) \implies \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)},$$

so just use polynomial long division.

**Lemma:**

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$
$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + \cdots - x + 1.$$

**Lemma:**

$$k \mid n \implies \Phi_{nk}(x) = \Phi_n\left(x^k\right)$$

**Theorem:** $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$ and is generated by maps of the form $\zeta_n \mapsto \zeta_n^j$ where $(j, n) = 1$.

## 3.2 Finite Fields

**Theorem:** $\mathbb{GF}(p^n)$ is obtained as $\dfrac{\mathbb{F}_p}{\langle f \rangle}$ where $f \in \mathbb{F}_p[x]$ is irreducible of degree $n$.

**Eisenstein's Criterion:** If $f(x) = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{Q}[x]$ and $\exists p$ such that

- $p \nmid a_n$ but $p \mid a_{i \neq n}$, and
- $p^2 \nmid a_0$,

then $f$ is irreducible.

## 3.3 Galois Theory

**Definition:** A field extension $L/k$ is **algebraic** iff every $\alpha \in L$ is the root of some $f \in k[x]$.

**Definition:** A field extension $L/k$ is **normal** iff

- Every embedding $\sigma : L \hookrightarrow \overline{k}$ that is a lift of the identity over $k$ satisfies $\sigma(L) = L$.
- Every irreducible $f \in k[x]$ that has one root in $L$ has all of its roots in $L$
- If $L$ is separable: $L$ is the splitting field of some irreducible $f \in k[x]$.

**Definition:** A field extension $L/k$ is **separable** iff

- For every $\alpha \in L, f(x) \coloneqq \min(\alpha, k)$ equivalently has
  - No repeated factors/roots
  - $f' \not\equiv 0$, or
  - $\gcd(f, f') = 1$.

**Lemma:** If char $k = 0$ or $k$ is finite, then every *algebraic* extension $L/k$ is separable.

**Definition:** Let $L/k$ be a finite field extension. TFAE:

- $L/k$ is **Galois**
- $L/k$ is normal and separable.
- $L/k$ is the splitting field of a separable polynomial
- $|\mathrm{Aut}(L/k)| = [L : k]$

**Lemmas about towers:** Let $L/F/k$ be a tower of field extensions

- $L/k$ normal $\implies$ $L/F$ normal.
- $L/k$ Galois $\implies$ $L/F$ Galois.
- $F/k$ is Galois $\iff$ $\mathrm{Gal}(L/F) \trianglelefteq \mathrm{Gal}(L/k)$
  - $\implies$ $\mathrm{Gal}(F/k) \cong \dfrac{\mathrm{Gal}(L/k)}{\mathrm{Gal}(L/F)}$
- **Every** quadratic extension is Galois.