MAT205: Abstract Algebra II

6. Classification of F.G. Abelian Groups and Applications

Ma, Jia-Jun – Xiamen University Malaysia

Recap of Lecture 5

Setup. F a free abelian group of rank n, $K \leq F$ a subgroup.

Subgroup Theorem (proved last lecture). There exists a basis $\{x_1, \ldots, x_n\}$ of F and positive integers $d_1 \mid d_2 \mid \cdots \mid d_s$ (with $s \leq n$) such that $\{d_1 x_1, \ldots, d_s x_s\}$ is a basis of K. In particular,

$$F/K \;\cong\; \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \oplus \mathbb{Z}^{n-s}.$$

This lecture. We (1) prove the d_i are **unique**, (2) reformulate everything via **Smith Normal Form**, (3) deduce the **Fundamental Theorem of Finitely Generated Abelian Groups**, (4) see applications ranging from $(\mathbb{Z}/n\mathbb{Z})^\times$ to the Birch–Swinnerton-Dyer conjecture.

Why Are the d_i Unique? – The d_i Live in F/K

Key observation. The subgroup theorem gives

$$F/K \;\cong\; \mathbb{Z}^{n-s} \oplus \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2 \oplus \cdots \oplus \mathbb{Z}/d_s.$$

The left-hand side is built directly from K – **no choice of basis, no matrix**. So whatever $(s; d_1, \ldots, d_s)$ is, it must be readable off from the group F/K itself.

Uniqueness reduces to: *can a finite abelian group $A \cong \bigoplus \mathbb{Z}/d_i$ have two different invariant-factor tuples?* We show the answer is **no**, by giving intrinsic formulas for each piece.

Free vs. torsion split. Let

$$A = (F/K)_{\text{tors}}$$

be the torsion subgroup. The quotient $(F/K)/A$ is free abelian, and

$$n - s \;=\; \operatorname{rank}\big((F/K)/A\big),$$

Recovering the d_i: Count m-Torsion

Notation. For an abelian group B, define the m-torsion subgroup by

$$T_m(B) \;=\; [B]_m \;:=\; \{b \in B : mb = 0\}.$$

Simple intrinsic data. For each $m \geq 1$, count:

$$N_m \;:=\; |T_m(A)| \;=\; |[A]_m|.$$

This depends only on the group A, not on any decomposition.

Easy formula in invariant form. In $\mathbb{Z}/d_i$, exactly $\gcd(m, d_i)$ elements satisfy $mt = 0$. So

$$N_m \;=\; \prod_{i=1}^{s} \gcd(m, d_i).$$

Recovering Every d_i

Fix a prime p. Since $d_1 \mid \cdots \mid d_s$, the valuations $v_p(d_1) \le \cdots \le v_p(d_s)$ are sorted. We recover them from the intrinsic counts N_m.

Intrinsic p-rank. Let $r_k(p) = \#\{i : p^k \mid d_i\}$. From $N_m = \prod_i \gcd(m, d_i)$,

$$\frac{N_{p^k}}{N_{p^{k-1}}} = p^{\,r_k(p)} \quad \Longrightarrow \quad r_k(p) \text{ is intrinsic.}$$

Pin down valuations. $\#\{i : v_p(d_i) = k\} = r_k(p) - r_{k+1}(p)$ is intrinsic, so the **multiset** $\{v_p(d_i)\}$ is determined by T. Sorted multiset $=$ the sorted sequence, so each $v_p(d_i)$ is determined. Combining over primes,

$$d_i = \prod_p p^{v_p(d_i)} \quad \text{is determined.} \qquad \blacksquare$$

Smith Normal Form

Theorem (SNF). Any integer matrix $A \in M_{m\times n}(\mathbb{Z})$ factors as

$$A \;=\; U \cdot D \cdot V, \qquad U \in GL_m(\mathbb{Z}),\; V \in GL_n(\mathbb{Z}),$$

where D is diagonal with entries $d_1 \mid d_2 \mid \cdots \mid d_r$ (the rest zero). The d_i are **unique**.

Allowed operations = swap rows/columns, negate a row/column, add an integer multiple of one row/column to another. These generate $GL_m(\mathbb{Z}) \times GL_n(\mathbb{Z})$.

Matrix form of the subgroup theorem. If columns of A generate $H \le \mathbb{Z}^n$, then row ops = change of basis of $\mathbb{Z}^n$, column ops = change of generators, and the SNF reads off the stacked basis:

$$\mathbb{Z}^n/H \;\cong\; \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_r \oplus \mathbb{Z}^{n-r}.$$

Henry J.S. Smith (1826–1883)

Irish-born British mathematician. **Savilian Professor of Geometry** at Oxford from 1861 until his death.

Key contributions.

- Theorem on **elementary divisors** of integer matrices (1861) — what we now call **Smith Normal Form**.
- Foundational work on **integer quadratic forms**; his ideas feed into the **Smith–Minkowski–Siegel mass formula**.
- Celebrated *Report on the Theory of Numbers* (1859–1865).

Honors. *Steiner Prize*, Berlin Academy, 1868. *Grand Prix des Sciences Mathématiques*, Paris Academy, 1882 — shared posthumously, for a problem on sums of five squares he had solved 15 years earlier.

Aside. Constructed the **Smith–Volterra–Cantor set** in 1875, predating Cantor's 1883 construction.

The Fundamental Theorem

Theorem (F.G. Abelian Groups). Every finitely generated abelian group G is isomorphic to

$$G \;\cong\; \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}, \qquad r \geq 0,\; d_i \geq 2,\; d_1 \mid \cdots \mid d_k.$$

The tuple $(r; d_1, \ldots, d_k)$ – the **invariants** of G – is unique. The isomorphism itself is not (e.g. $\mathbf{Aut}(\mathbb{Z}^r) = GL_r(\mathbb{Z})$).

Vocabulary. r = free rank (Betti number); $G_{\text{tors}} = \bigoplus \mathbb{Z}/d_i$ = torsion subgroup; the d_i are the **invariant factors**.

Proof. Pick generators $g_1, \ldots, g_n$, get a surjection $\pi : \mathbb{Z}^n \twoheadrightarrow G$, so $G \cong \mathbb{Z}^n / \ker \pi$. Apply the stacked-basis theorem to $\ker \pi$: some basis of $\mathbb{Z}^n$ gives $\ker \pi = \langle d_1 v_1, \ldots, d_m v_m \rangle$, hence

$$G \;\cong\; \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_m \oplus \mathbb{Z}^{n-m}. \qquad \square$$

Primary Decomposition

Theorem. Every finite abelian group splits **canonically** as a direct sum over primes:

$$G \;=\; \bigoplus_{p} T_{p^\infty}(G).$$

Here

$$T_{p^\infty}(G) \;:=\; \{\, g \in G : p^k g = 0 \text{ for some } k \geq 1 \,\}.$$

$T_{p^\infty}(G)$ is the **p-power torsion** of G – equivalently, its p-Sylow subgroup. It is defined **directly from G**: no basis, no choices. Hence the splitting is literally an equality of subgroups of G, not just an isomorphism.

Inside Each Primary Part

Apply the classification theorem to the p-group $T_{p^\infty}(G)$.

Then

$$T_{p^\infty}(G) \cong \bigoplus_{j=1}^{s_p} \mathbb{Z}/p^{a_{p,j}}\mathbb{Z},$$

where

$$1 \leq a_{p,1} \leq \cdots \leq a_{p,s_p}.$$

The partition $(a_{p,j})_j$ is **unique**.

The specific cyclic summands require a basis.

Invariant Factors vs. Primary Decomposition

Two equivalent ways to classify a finite abelian group G:

Invariant factors. $G \cong \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_k$ with $d_1 \mid \cdots \mid d_k$.

- Minimal description – fewest cyclic summands.
- Largest factor is the exponent: $d_k = \exp(G)$.

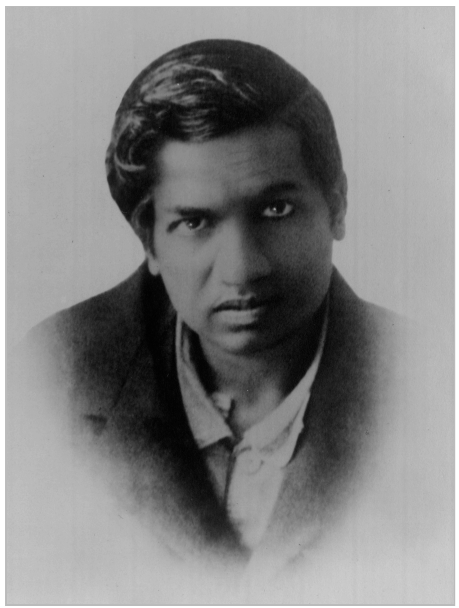
Primary decomposition. $G = \bigoplus_p T_{p^\infty}(G)$, each $T_{p^\infty}(G) \cong \bigoplus_j \mathbb{Z}/p^{a_{p,j}}\mathbb{Z}$.

- **Canonical** at the top level ($T_{p^\infty}(G)$ = p-power torsion).
- Separates arithmetic by prime – the natural form for counting, p-local questions, and anything involving Sylow subgroups.

Translating between them. Write each $d_i = \prod_p p^{e_{p,i}}$. Then the partition $(a_{p,j})_j$ is the multiset of nonzero valuations $\{e_{p,i} : e_{p,i} > 0\}_i$, sorted. Going back: d_k picks the largest $p^{a_{p,s_p}}$ from each prime, then d_{k-1} picks the next-largest, and so on.

Aside: Partitions and Ramanujan

Counting abelian groups of order p^n = counting **partitions** of n (the exponent tuples $a_{p,1} \le \cdots \le a_{p,s_p}$). This connects the classification to a deep strand of number theory.



Srinivasa Ramanujan (1887–1920). Self-taught Indian mathematician; came to Cambridge on Hardy's invitation in 1914. Died at 32. Left three notebooks containing ~3900 identities, many still being unpacked today.

Partition function. $p(n)$ = number of ways to write n as a sum of positive integers (order ignored).

$$p(1),\ p(2),\ p(3),\ p(4),\ p(5),\ \ldots\ =\ 1,\ 2,\ 3,\ 5,\ 7,\ 11,\ 15,\ 22,\ 30,\ldots$$

Euler's generating function (1748):

$$\sum_{n\ge 0} p(n)\,q^n\ =\ \prod_{k\ge 1}\frac{1}{1-q^k}.$$

Ramanujan on Partitions

Hardy–Ramanujan asymptotic (1918). $p(n)$ grows almost exponentially:

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\tfrac{2n}{3}}\right) \quad \text{as } n \to \infty.$$

Proved via the **circle method**; later sharpened by Rademacher into an exact convergent series.

Ramanujan congruences. Despite $p(n)$ being "wild," it has mysterious arithmetic regularity:

$$p(5n+4) \equiv 0 \pmod 5, \qquad p(7n+5) \equiv 0 \pmod 7, \qquad p(11n+6) \equiv 0 \pmod{11}.$$

No such nice congruences for other primes $\ell \leq 23$ – and the full pattern was only explained by **Ono** (2000) via modular forms.

Check. $p(4) = 5$: partitions $4,\ 3{+}1,\ 2{+}2,\ 2{+}1{+}1,\ 1{+}1{+}1{+}1$. And $5 \equiv 0 \pmod 5$. ✓

Lens for us. Abelian p-groups of order p^n are counted by $p(n)$ – so their count grows almost exponentially in n.

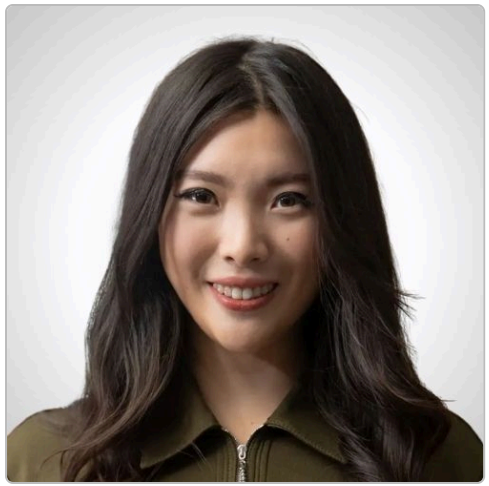
Aside: Ken Ono and Axiom Math

Ken Ono (b. 1968). American number theorist. Ph.D. UCLA 1993 (advisor: Basil Gordon). Long career at Wisconsin, Emory, and most recently **Thomas Jefferson Professor** at the University of Virginia. Ph.D. advisor to many of today's leading number theorists.

Selected results.

- **Partition congruences (2000).** Proved, with Ahlgren, that for **every** prime $\ell \geq 5$ there exist infinitely many Ramanujan-type congruences $p(An + B) \equiv 0 \pmod{\ell}$ – via modular forms, finally explaining Ramanujan's mod $5, 7, 11$ as the tip of a much larger iceberg.
- **Umbral moonshine** (2015, with Duncan & Griffin): generalizing monstrous moonshine.
- **Jensen–Pólya criterion** (2019): substantial progress toward the Riemann Hypothesis.
- Scientific consultant on *The Man Who Knew Infinity* (2015), the Ramanujan biopic.

Axiom Math — and Carina Hong



Carina Hong (b. ~2001). Chinese-born mathematician. Guangdong olympiad team; **dual MIT degrees in Math & Physics in 3 years**, with 9 peer-reviewed papers as an undergrad. **Morgan Prize 2023** (top U.S. prize for an undergrad mathematician); **Rhodes Scholar** → Oxford MSc (Neuroscience / deep learning); started Stanford math Ph.D., then **dropped out in early 2025** to found **Axiom Math**. Axiom: **$64M seed** (Sept 2025), then **$200M at $1.6B+** (Menlo Ventures). Team ~17 from Meta FAIR, Google Brain, DeepMind.

Axiom's goal — "the starting point for reasoning". An AI mathematician that **reasons**, **conjectures**, and **verifies** its own proofs in a formal proof system (Lean / Coq-style). Ono leads math direction; Hong runs the company.

Why it lands here. The formal-proof leg is exactly what this course's Lean-based game trains you to do.

Example: Abelian Groups of Order 8

$8 = 2^3$. Partitions of 3 (listing exponents of $\mathbb{Z}/2^{a_i}$):

Partition	Primary decomposition	Invariant factors
3	$\mathbb{Z}/8$	$d_1 = 8$
$2+1$	$\mathbb{Z}/4 \oplus \mathbb{Z}/2$	$d_1 = 2, d_2 = 4$
$1+1+1$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$	$d_1 = 2, d_2 = 2, d_3 = 2$

So there are exactly **3** abelian groups of order 8 up to isomorphism.

(Compare with total count: 5 groups of order 8 – 3 abelian + D_4 + Q_8.)

Example: Abelian Groups of Order 12

$12 = 2^2 \cdot 3$. Decompose each prime part separately.

2-part: partitions of 2 – either $\mathbb{Z}/4$ or $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.

3-part: partition of 1 – only $\mathbb{Z}/3$.

Combine:

Primary	Invariant factors	Cyclic?
$\mathbb{Z}/4 \oplus \mathbb{Z}/3$	$d_1 = 12$	$\mathbb{Z}/12$ ✓
$\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3$	$d_1 = 2, d_2 = 6$	–

So there are exactly **2** abelian groups of order 12.

(Compare with total: 5 groups of order 12 – 2 abelian + A_4 + D_6 + Dic_3.)

Example: Abelian Groups of Order 360

$360 = 2^3 \cdot 3^2 \cdot 5$. Count partitions:

- 2^3: partitions of 3 → 3 options ($3;\ 2{+}1;\ 1{+}1{+}1$)
- 3^2: partitions of 2 → 2 options ($2;\ 1{+}1$)
- 5^1: partitions of 1 → 1 option

Total: $3 \times 2 \times 1 = 6$ abelian groups of order 360.

Formula. The number of abelian groups of order $n = \prod p_i^{a_i}$ is

$$\prod_i p(a_i)$$

where $p(a)$ is the number of partitions of a.

Uniqueness via Invariants

How do we know two f.g. abelian groups are distinct?

Invariants to compute:

1. **Free rank** r: largest r such that $G \supseteq \mathbb{Z}^r$ (equivalently, rank of G/G_{tors}).
2. **Torsion subgroup**: $G_{\text{tors}} = \{g \in G \mid ng = 0 \text{ for some } n > 0\}$.
3. **p-primary part**: $T_{p^\infty}(G) = \{g \mid p^k g = 0 \text{ for some } k \geq 1\}$.
4. **p-rank**: $\dim_{\mathbb{F}_p} T_p(G)$, where $T_p(G) = [G]_p = \{g \mid pg = 0\}$.

Example. $\mathbb{Z}/4 \oplus \mathbb{Z}/2$ vs $\mathbb{Z}/2^3$: both order 8 and 2-groups, but

$$T_2(\mathbb{Z}/4 \oplus \mathbb{Z}/2) = [\mathbb{Z}/4 \oplus \mathbb{Z}/2]_2 \cong (\mathbb{Z}/2)^2,$$

while $T_2(\mathbb{Z}/8) \cong \mathbb{Z}/2$. The 2-ranks differ, so they are **not isomorphic**. ✓

Application: Elliptic Curves

An **elliptic curve** over $\mathbb{Q}$ is a smooth cubic $E : y^2 = x^3 + ax + b$ (with nonzero discriminant). The set of rational solutions, plus a "point at infinity," forms an abelian group $E(\mathbb{Q})$ under the chord-and-tangent addition.

Mordell–Weil Theorem (1928). $E(\mathbb{Q})$ is a **finitely generated** abelian group. By our classification:

$$E(\mathbb{Q}) \;\cong\; \mathbb{Z}^r \;\oplus\; E(\mathbb{Q})_{\text{tors}}.$$

- **Rank** r – the big unknown. No algorithm is known for computing it; examples with $r \geq 28$ exist but it's open whether r is bounded.
- **Torsion** $E(\mathbb{Q})_{\text{tors}}$ – **Mazur's theorem** (1977): only 15 possibilities, all cyclic $\mathbb{Z}/n$ ($n \in \{1, \ldots, 10, 12\}$) or $\mathbb{Z}/2 \oplus \mathbb{Z}/2m$ ($m \in \{1, 2, 3, 4\}$).
- **Tate–Shafarevich group** $Ш(E/\mathbb{Q})$ – a (conjecturally finite) abelian group measuring failure of local-to-global principles. Studied via the same $T_p(A) = [A]_p$, p-rank, and primary-decomposition tools as in this lecture.

Louis Mordell (1888–1972)

American-born (**Philadelphia, 1888**), became a British citizen in 1929. Trained at **St John's College, Cambridge** (Third Wrangler, 1909). Held the **Fielden Chair** at Manchester (1920–1945), then the **Sadleirian Chair** of Pure Mathematics at Cambridge (1945–1953).

Mordell's Theorem (1922). For an elliptic curve $E/\mathbb{Q}$, the group $E(\mathbb{Q})$ is **finitely generated** — resolving a question posed by Poincaré (1901). This is the rank-r side of our lecture's classification applied to a deep arithmetic object.

Mordell conjecture (1922). Curves of genus ≥ 2 over $\mathbb{Q}$ have only finitely many rational points. Open for 60 years; finally proved by **Faltings** (1983) — who won the Fields Medal for it.

Honors. De Morgan Medal (1941), Sylvester Medal (1949), FRS.

Faltings and the 2026 Abel Prize

Gerd Faltings (b. 1954, Germany). In **1983**, at age 28, he proved the Mordell conjecture using sweeping new tools in arithmetic geometry. **Fields Medal 1986.** Director of the **Max Planck Institute for Mathematics**, Bonn (1994–2018).

Niels Henrik Abel (1802–1829). Norwegian, died of tuberculosis at 26. Proved the **unsolvability of the general quintic** by radicals (1824). **Commutative groups bear his name** – they are *abelian* groups.

Abel Prize 2026 (announced this March) – "*for introducing powerful tools in arithmetic geometry and resolving long-standing diophantine conjectures of Mordell and Lang.*" First German Abel laureate; ceremony in Oslo on May 26, 2026.

The Abel Prize (established 2002) is awarded annually by the Norwegian Academy – often called the "Nobel of mathematics." Past laureates include Serre, Atiyah & Singer, Tate, Deligne, Wiles, Langlands, Margulis… and now Faltings.

André Weil (1906–1998)

French mathematician. **ENS Paris**; Ph.D. Paris 1928. Founding member of **Bourbaki**. Career at São Paulo, **Chicago** (1947–58), and finally at the **Institute for Advanced Study** in Princeton.

Mordell–Weil Theorem (1929). Extended Mordell's theorem from $\mathbb{Q}$ to any number field K – and from elliptic curves to any abelian variety A/K: $A(K)$ is finitely generated. Our structure theorem gives $A(K) \cong \mathbb{Z}^r \oplus A(K)_{\text{tors}}$.

Weil conjectures (1949). Predicted deep properties of zeta functions of varieties over finite fields – rationality, functional equation, "Riemann hypothesis." Inspired the development of **étale cohomology** (Grothendieck) and were fully proved by **Deligne** (1974).

Honors. Wolf Prize (1979), Kyoto Prize (1994), FRS (1966).

The Birch–Swinnerton-Dyer Conjecture

No algorithm is known to compute the rank r. But there is a **conjectural formula** relating r to an **L-function** $L(E, s)$ built from counting E over every $\mathbb{F}_p$:

$$L(E, s) \;=\; \prod_{p \text{ good}} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}, \qquad a_p = p + 1 - \#E(\mathbb{F}_p).$$

$L(E, s)$ extends meromorphically to $\mathbb{C}$ (Wiles, Breuil–Conrad–Diamond–Taylor).

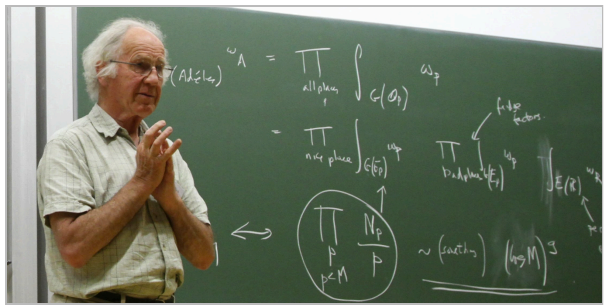
Weak BSD. $\operatorname{ord}_{s=1} L(E, s) \;=\; r$ (analytic rank = algebraic rank).

Strong BSD. The leading Taylor coefficient at $s = 1$ is

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} \;=\; \frac{\Omega_E \cdot \operatorname{Reg}(E) \cdot |Ш(E)| \cdot \prod_p c_p}{|E(\mathbb{Q})_{\text{tors}}|^2}.$$

One of the **Clay Millennium Problems** ($1M). Partial cases known – analytic rank 0 and 1 (Gross–Zagier, Kolyvagin).

Who Are Birch and Swinnerton-Dyer?



Bryan John Birch (b. 1931). British; Ph.D. Cambridge 1958 under J.W.S. Cassels. Long career at **Oxford**. Honors: FRS (1972), Senior Whitehead Prize (1993), De Morgan Medal (2007), Sylvester Medal (2020).

Sir Peter Swinnerton-Dyer (1927–2018). British; Ph.D. Cambridge under Littlewood and Weil. **Trinity College**, Cambridge — later Master of St Catharine's and Vice-Chancellor of Cambridge (1979–81). FRS (1967), KBE (1987).

The conjecture's origin. In the early **1960s**, Birch and Swinnerton-Dyer ran numerical experiments on the **EDSAC 2** computer at Cambridge, tabulating $\prod_{p \le X} \#E(\mathbb{F}_p)/p$ for many elliptic curves. They noticed the growth rate depended on r — leading to the formula now bearing their names. It remains one of the deepest open problems in mathematics.

Application: Finite Subgroups of a Field Are Cyclic

Theorem. Let K be a field and $G \leq K^\times$ a finite subgroup. Then G is cyclic.

Proof. By the classification, $G \cong \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_k$ with $d_1 \mid \cdots \mid d_k$. Every $x \in G$ satisfies $x^{d_k} = 1$ (the exponent).

In a field, $X^{d_k} - 1$ has at most d_k roots, so $|G| \leq d_k$. But $|G| = d_1 d_2 \cdots d_k$, which forces $d_1 = \cdots = d_{k-1} = 1$. Hence $G \cong \mathbb{Z}/d_k$. $\blacksquare$

Corollaries.

- $(\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ – primitive roots exist mod every prime.
- $\mathbb{F}_q^\times$ is cyclic for every finite field $\mathbb{F}_q$.
- Every finite subgroup of $\mathbb{C}^\times$ is a group of n-th roots of unity.

Application: Structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

The unit group $(\mathbb{Z}/n\mathbb{Z})^\times$ is a finite abelian group – our theorem applies.

CRT: $(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_p (\mathbb{Z}/p^{a_p}\mathbb{Z})^\times$ where $n = \prod p^{a_p}$.

Structure theorem for $(\mathbb{Z}/p^a\mathbb{Z})^\times$:

- p odd: $(\mathbb{Z}/p^a\mathbb{Z})^\times \cong \mathbb{Z}/p^{a-1}(p-1)\mathbb{Z}$ – **cyclic**
- $p = 2, a \geq 3$: $(\mathbb{Z}/2^a\mathbb{Z})^\times \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2^{a-2}$
- $p = 2, a \leq 2$: $(\mathbb{Z}/2)^\times = 1, (\mathbb{Z}/4)^\times \cong \mathbb{Z}/2$

Example. $(\mathbb{Z}/12)^\times = (\mathbb{Z}/4)^\times \times (\mathbb{Z}/3)^\times \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ – **Klein 4-group**, not cyclic.

Proof Sketch (I): Split via Reduction

Fix a prime power p^a. We want to understand $(\mathbb{Z}/p^a)^\times$, a group of order $\phi(p^a) = p^{a-1}(p-1)$.

Reduction map. $\pi : (\mathbb{Z}/p^a)^\times \twoheadrightarrow (\mathbb{Z}/p)^\times$, sending $x \mapsto x \bmod p$.

- **Kernel** = $U_1 := \{1 + px : x \in \mathbb{Z}/p^{a-1}\mathbb{Z}\}$, the **principal units**. $|U_1| = p^{a-1}$.
- **Image** = $(\mathbb{Z}/p)^\times$, cyclic of order $p-1$ (finite subgroup of $\mathbb{F}_p^\times$ – previous slide).

Split. The short exact sequence $1 \to U_1 \to (\mathbb{Z}/p^a)^\times \to (\mathbb{Z}/p)^\times \to 1$ splits:

- Orders p^{a-1} and $p-1$ are **coprime**, and both groups are finite abelian – any such extension splits (e.g. by Schur–Zassenhaus, or directly: the $p-1$-power map retracts onto a subgroup complementary to U_1).

$$(\mathbb{Z}/p^a)^\times \;\cong\; U_1 \;\times\; (\mathbb{Z}/p)^\times.$$

Reduced question. What is the structure of U_1? This is controlled by how p-th powering shifts p-adic valuations.

Proof Sketch (II): The p-adic Lemma (Odd p)

Lemma. Let p be an odd prime, $k \geq 1$, and c an integer with $p \nmid c$. Then

$$(1 + c\,p^k)^p \;\equiv\; 1 + c\,p^{k+1} \pmod{p^{k+2}}.$$

Proof. Binomial expansion:

$$(1 + cp^k)^p \;=\; 1 \;+\; p \cdot cp^k \;+\; \binom{p}{2}(cp^k)^2 \;+\; \sum_{j \geq 3} \binom{p}{j}(cp^k)^j.$$

- $p \cdot cp^k = cp^{k+1}$ – the main correction term. ✓
- $\binom{p}{2} = \frac{p(p-1)}{2}$ has **one factor of p** (since p odd, 2 is invertible mod p). So $\binom{p}{2}(cp^k)^2$ has valuation $\geq 1 + 2k \geq k + 2$.
- For $j \geq 3$: valuation $\geq jk \geq 3k \geq k + 2$ when $k \geq 1$.

Everything after the main term has valuation $\geq k + 2$. $\square$

Proof Sketch (II'): Odd p – Finishing Up

By iterating the lemma j times starting at $k = 1$:

$$(1+p)^{p^j} \equiv 1 + p^{j+1} \pmod{p^{j+2}}.$$

Order of $1+p$ in $(\mathbb{Z}/p^a)^\times$.

- $(1+p)^{p^{a-2}} \equiv 1 + p^{a-1} \not\equiv 1 \pmod{p^a}$ – order isn't p^{a-2}.
- $(1+p)^{p^{a-1}} \equiv 1 + p^a \equiv 1 \pmod{p^a}$ – order divides p^{a-1}.

Hence $\operatorname{ord}(1+p) = p^{a-1} = |U_1|$.

So $U_1 = \langle 1+p \rangle$ is **cyclic** of order p^{a-1}. Combined with Part I and $\gcd(p^{a-1}, p-1) = 1$:

$$(\mathbb{Z}/p^a)^\times \cong U_1 \times (\mathbb{Z}/p)^\times \cong \mathbb{Z}/p^{a-1}(p-1)\mathbb{Z}. \qquad \blacksquare$$

Proof Sketch (III): The $p = 2$ Exception

Why $p = 2$ is special. The lemma used $p \mid \binom{p}{2}$. For $p = 2$, $\binom{2}{2} = 1$ – no extra factor of 2. Recompute:

$$(1 + 2^k)^2 \;=\; 1 + 2^{k+1} + 2^{2k} \;\equiv\; 1 + 2^{k+1} \pmod{2^{k+2}} \quad (k \geq 2).$$

So the lemma works only **starting from $k = 2$**: begin with $1 + 4 = 5$.

Consequence. $\operatorname{ord}(5) = 2^{a-2}$ in $(\mathbb{Z}/2^a)^\times$ for $a \geq 2$. So $\langle 5 \rangle$ has order 2^{a-2}, but $|U_1| = 2^{a-1}$ – **off by a factor of 2**.

The missing factor is -1. Every power of 5 is $\equiv 1 \pmod 4$, but $-1 \equiv 3 \pmod 4$ – so $-1 \notin \langle 5 \rangle$. Hence $\langle -1 \rangle \cap \langle 5 \rangle = \{1\}$, and their product has order $2 \cdot 2^{a-2} = |U_1|$:

$$(\mathbb{Z}/2^a)^\times \;=\; \langle -1 \rangle \times \langle 5 \rangle \;\cong\; \mathbb{Z}/2 \oplus \mathbb{Z}/2^{a-2} \quad (a \geq 3). \qquad \blacksquare$$

Summary

Concept	Key result
Uniqueness of d_i	d_i are invariants of $G = F/K$; recovered from $N_m = \lvert T_m(G)\rvert = \lvert[G]_m\rvert$
Smith Normal Form	Any integer matrix $= UDV$ with D diagonal, $d_1 \mid \cdots \mid d_r$
Fundamental Theorem	$G \cong \mathbb{Z}^r \oplus \bigoplus \mathbb{Z}/d_i\mathbb{Z}$, $d_1 \mid \cdots \mid d_k$, unique
Primary form	$G = \bigoplus_p T_{p^\infty}(G)$, each $T_{p^\infty}(G) \cong \bigoplus_j \mathbb{Z}/p^{a_{p,j}}\mathbb{Z}$
Units mod n	$(\mathbb{Z}/p^a)^\times$ cyclic for odd p; $\mathbb{Z}/2 \oplus \mathbb{Z}/2^{a-2}$ for $p = 2, a \geq 3$
Finite subgroups of a field	Always cyclic
Elliptic curves	$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$ (Mordell–Weil); rank r = BSD

The big picture. Finitely generated abelian groups reduce to linear algebra over $\mathbb{Z}$ via Smith Normal Form.

Looking Ahead

Next (Lecture 7): Composition series and solvable groups.

- Jordan–Hölder theorem: every finite group has a well-defined "composition series"
- Solvable groups: those whose composition factors are all abelian
- This is where **simple groups** (A_5!) become unavoidable

Later in the course. The same ideas generalize to modules over PIDs, and eventually lead to the classification of finitely generated modules over polynomial rings — the theory behind rational / Jordan canonical form in linear algebra.

Homework (Lecture 6)

Exercise 1. List all abelian groups of order 72 up to isomorphism, giving both the invariant-factor form and the primary decomposition.

Exercise 2. Let $G \cong \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}$ and define

$$T_d(G) = [G]_d = \{g \in G : dg = 0\}.$$

Prove

$$|T_d(G)| = |[G]_d| = \prod_i \gcd(d, d_i),$$

and count the elements of order exactly 4 in $\mathbb{Z}/4 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/8$.

Exercise 3. Compute the structure of $(\mathbb{Z}/105\mathbb{Z})^\times$ as an abelian group. (Hint: CRT + structure of $(\mathbb{Z}/p^a)^\times$.)

Questions?