Honors Algebra II Final Review

Rohan Buluswar

March 2025

1 Rings and Ideals

Definition 1.1 (**Rings**). *A ring R is a set with binary operations $+$ and $\times$ such that:*

- $(R, +)$ *is an abelian group*
- $\times : R \times R \to R$ *is associative*
- $(a + b) \times c = (a \times c) + (b \times c)$ *and* $a \times (b + c) = (a \times b) + (a \times c)$ *for all* $a, b, c \in R$

Definition 1.2 (**Abelian rings**). *A ring R is called abelian, or commutative, if for all $a, b \in R$, $ab = ba$.*

Definition 1.3. *A ring R is said to have identity if there exists an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.*

Definition 1.4. *A ring R with identity is called a division ring if for all $a \neq 0 \in R$, there exists $b \in R$ such that $ab = ba = 1$.*

Proposition 1.1. *If R is any ring,*

- $0 \times a = a \times 0 = 0$ *for all* $a \in R$
- $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$
- $(-a)(-b) = ab$ *for all* $a, b \in R$
- *If* $1 \in R$*, then it is unique and* $-a = (-1)a$ *for all* $a \in R$

Definition 1.5 (**Zero divisors, units**). *An element $a \in R$ is called a zero divisor if $a \neq 0$ and there exists $b \neq 0 \in R$ such that $ab = 0$ or $ba = 0$. If R has $1 \in R$. then $u \in R$ is called a unit if there exists $v \in R$ such that $uv = vu = 1$. The set of units is denoted by $R^\times$.*

Definition 1.6 (**Integral domain**). *If R is abelian, has no zero divisors, and $1 \in R$, we call R an integral domain.*

Proposition 1.2. *If R is an integral domain and $a \neq 0$, then $ab = ac \implies b = c$.*

Proposition 1.3. *A finite integral domain R is a field.*

Definition 1.7 (**Subring**). *A subring of R is a subgroup w.r.t $+$ that is also closed under multiplication.*

Definition 1.8 (**Ring homomorphism**). *Let R, S be rings and let $\varphi : R \to S$ be a function. It is called a homomorphism if for all $a, b \in R$,*

$$\varphi(a +_R b) = \varphi(a) +_S \varphi(b) \in S$$

$$\varphi(a \times_R b) = \varphi(a) \times_S \varphi(b) \in S$$

Definition 1.9 (**Kernel**). *The kernel of a homomorphism $\varphi : R \to S$ is defined as*

$$\ker(\varphi) = \{r \in R : \varphi(r) = 0 \in S\}$$

Definition 1.10 (**Isomorphism**). *If $\varphi : R \to S$ is a bijective homomorphism, then it is called an isomorphism. If such a φ exists between R and S, we say they are isomorphic and write $R \cong S$.*

Proposition 1.4. *If $\varphi : R \to S$ is a homomorphism then $\varphi(R) \subseteq S$ is a subring and $\ker(\varphi) \subseteq R$ is a subring.*

Definition 1.11 (**Ideals**). *A subset $I \subseteq R$ is called a left ideal if I is a subring of R and for all $i \in I, r \in R$, $ri \in I$. That is, $rI \subseteq I$. I is instead called a right ideal if it is a subring and $Ir \subseteq I$ for all $r \in R$. If I is both a left and right ideal, it is simply called a (two-sided) ideal.*

Definition 1.12 (**Quotient ring**). *If $I \subseteq R$ is an ideal, we define a quotient ring R/I by*

$$(r + I) + (s + I) = (r + s) + I$$

$$(r + I)(s + I) = (rs) + I$$

(Note that because the group structure of R is additive, the cosets are denoted by addition.)

Theorem 1.1 (**First Isomorphism Theorem**). *If $\varphi : R \to S$ is a homomorphism, then $\ker(\varphi) \subseteq R$ is an ideal and*

$$R/\ker(\varphi) \cong \varphi(R)$$

Theorem 1.2 (**Second Isomorphism Theorem**). *Let $A \subseteq R$ be a subring and let $B \subseteq R$ be an ideal. Then $A + B$ is a subring and*

$$(A + B)/B \cong A/(A \cap B)$$

Theorem 1.3 (**Third Isomorphism Theorem**). *If $I \subseteq J \subseteq R$ are ideals then*

$$(R/I) \Big/ (J/I)$$

Theorem 1.4 (**Fourth Isomorphism Theorem**). *If $I \subseteq R$ is an ideal, then the correspondence $A \longleftrightarrow A/I$ is an inclusion-preserving bijection between subrings of R/I and subrings A of R that contain I. Moreover, $A \subseteq R$ is an ideal iff $A/I \subseteq R/I$ is an ideal.*

Definition 1.13. *If $I, J \subseteq R$, we define*

$$I + J = \{a + b | a \in I, b \in J\}$$

$$IJ = \{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J\}$$

Definition 1.14. *If $A \subseteq R$, let (A) denote the smallest ideal containing A, i.e. the ideal generated by A. If $|A| = 1$, the ideal (A) is called principal. (Note: generators need not be unique.)*

Remark: If R is commutative, then $(ab) = (a)(b)$.

Definition 1.15. *We introduce the following notation:*

$$RA = \{a_1r_1 + \ldots + a_nr_n | r_i \in R, a_i \in A\}$$

and similarly for AR and RAR.

Remark: RA is the left-ideal generated by A, and AR is the right-ideal. Thus, if R is abelian, then $(A) = AR = RA$.

Proposition 1.5. *Let $I \subseteq R$ be an arbitrary ideal. Then*

- *$I = R$ iff I contains a unit*
- *If R is abelian, R is a field $\iff$ $I = R$ or $I = \{0\}$ (i.e. those are the only ideals)*

Definition 1.16. *Let $M \subsetneq R$ be an ideal such that if M' is an ideal and $M \subseteq M' \subseteq R$, then $M' = M$ or $M' = R$. Then M is called maximal.*

Definition 1.17. *If R has 1, every proper ideal is contained in a maximal ideal.*

Proposition 1.6. *If R is abelian, then an ideal M is maximal iff R/M is a field.*

Definition 1.18 (**Prime ideals**). *Suppose R is abelian. An ideal $P \subseteq R$ is called prime if $P \neq R$ and $ab \in P \implies a \in P$ or $b \in P$.*

Proposition 1.7. *If (p) is a prime ideal and $p = ab$, then a is a unit or b is a unit.*

Proposition 1.8. *Suppose R is abelian. Then an ideal P is prime iff R/P is an integral domain.*

Corollary 1.4.1. *If R is abelian, then all maximal ideals are prime.*

Theorem 1.5. *If R is abelian and we have $D \subseteq R$ that is closed under multiplication such that $D \neq \emptyset$ and $0 \notin D$, and D contains no zero divisors, then there exists a commutative ring Q with 1 such that $R \subseteq Q$ is a subring and for all $d \in D$, d is a unit in Q. Moreover, any $q \in Q$ has the form rd^{-1} for $r \in R$, $d \in D$. We call Q the ring of fractions.*

2 CRT, Euclidean Domains, and UFDs

Definition 2.1 (**Comaximal ideals**). *Ideals A, B are called comaximal if $A + B = R$.*

Lemma 2.1. *If R is commutative and $1 \in R$, then for ideals $I, J \subseteq R$, $I + J = R \implies IJ = I \cap J$.*

Theorem 2.2 (**Chinese Remainder Theorem**). *Let $A_1, A_2, \ldots, A_k \subseteq R$ be ideals. The map*

$$\varphi : R \to (R/A_1) \times \ldots \times (R/A_k)$$

defined by

$$\varphi : r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with

$$\ker(\varphi) = A_1 \cap A_2 \ldots \cap A_k$$

If for each $i \neq j$ we have $A_i + A_j = R$, i.e. the ideals are pairwise comaximal, then φ is surjective and

$$A_1 \cap A_2 \cap \ldots \cap A_k = A_1 A_2 \ldots A_k$$

so we conclude that

$$R/(A_1 \ldots A_k) = R/(A_1 \cap \ldots \cap A_k) \cong (R/A_1) \times \ldots \times (R/A_k)$$

Remark: φ is also an isomorphism of units.

Corollary 2.2.1. *If $n \in \mathbb{Z}$, then it can be factorized into distinct primes as $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Then by CRT,*

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

and

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$

Definition 2.2 (Norm). *Given a ring R, a function $N : R \to \mathbb{N}_{\geq 0}$ with $N(0) = 0$ is called a norm on R. If $a \neq 0 \implies N(a) > 0$, it is called positive.*

Definition 2.3 (Euclidean Domain). *An integral domain R is called a Euclidean domain if there exists a norm N on R such that for all $a, b \in R$ such that $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and $r = 0$ or $N(r) < N(b)$.*

Remark: This is the generalization of division with remainder and enables us to perform the Euclidean algorithm.

Proposition 2.1. *If R is a Euclidean domain and $I \subseteq R$ is a nonzero ideal, then $I = (d)$ where d is some nonzero element of I with minimum norm. That is, if R is a Euclidean domain then R is a PID.*

Definition 2.4 (Greatest common divisor). *Let R be commutative and let $a, b \in R$ such that $b \neq 0$. We say b divides a and write $b|a$ if $a = xb$ for some $x \in R$. A gcd of a and b is an element $d \neq 0$ such that $d|a, d|b$ and for any d' such that $d'|a$ and $d'|b$, we have $d'|d$. We write $d = (a, b)$.*

Alternatively, $d = (a, b)$ if $I = (a, b) \subseteq (d)$ and $I \subseteq (d') \implies (d) \subseteq (d')$.

Proposition 2.2. *If R is abelian and $(a, b) = (d)$, then $d = (a, b)$.*

Proposition 2.3. *If R is an integral domain and $(d) = (d')$, then $d' = ud$ for some unit u, and we say that the two are associate.*

Remark: The gcd is only unique up to multiplication by a unit.

Theorem 2.3. *Let $d = r_n$ be the least nonzero remainder in the Euclidean algorithm for a, b. Then $d = (a, b)$ and $d = ax + by$ for some $x, y \in R$.*

Proposition 2.4. *If $ax_0 + by_0 = N$ then all other solutions have the form $x = x_0 + m\frac{b}{(a,b)}$ and $y = y_0 - m\frac{a}{(a,b)}$.*

Proposition 2.5. *Every nonzero prime ideal in a PID is a maximal ideal.*

Definition 2.5 (**Irreducibility**). *Suppose $p \in R$ is an element such that for all factorizations $p = ab$, we have that a is a unit or b is a unit. Moreover, suppose that $p \neq 0$ and p is not a unit. Then p is called irreducible.*

Definition 2.6 (**Prime elements**). *Given $p \in R$ where R is an integral domain, suppose that $p \neq 0$ and p is not a unit. Then, if (p) is a prime ideal, we say that p itself is a prime element of R.*

Remark: We know in general that prime elements are irreducible. But the converse need not be true, as $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime.

Definition 2.7 (**Unique Factorization Domains**). *A UFD, or unique factorization domain, is an integral domain R in which any non-zero element $a \in R$ has a factorization into primes:*

$$a = p_1 p_2 \dots p_m$$

that is essentially unique. Specifically, if we also have

$$a = q_1 \dots q_n$$

where the q_j are prime, then $n = m$ and we can re-order the factors so that each p_i is associate to q_i.

Theorem 2.4. *Any PID is also a UFD. As a result, any Euclidean domain is also a UFD.*

Now, we have seen that Euclidean domain $\implies$ PID $\implies$ UFD.

Proposition 2.6. *If R is a PID (or more generally, a UFD), then all irreducible elements are prime.*

3 Polynomial Rings and Irreducibility

Definition 3.1 (**Polynomial rings**). *Given a ring R, we can define the ring of polynomials in a single variable x with coefficients in R as follows:*

$$R[x] = \{(a_0, a_1, \dots, a_n, \dots) | a_i \in R, \exists m \in \mathbb{N} : \forall n \geq m, a_n = 0\}$$

Addition is defined componentwise and multiplication is defined by convolution.

We can similarly define polynomial rings with more variables, like $R[x, y]$, etc.

Proposition 3.1. *Let R be an integral domain. Then*

- *For any nonzero $p, q \in R[x]$, $deg(pq) = deg(p) + deg(q)$*
- *The units of $R[x]$ are the units of R as constant polynomials*
- *$R[x]$ is an integral domain*

Proposition 3.2. *Let R be commutative with 1. If $I \subseteq R$ is an ideal then $IR[x] \subseteq R[x]$ is the ideal where all coefficients are in I. Then we have*

$$R[x]/IR[x] \cong (R/I)[x]$$

Example: If $R = \mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a Euclidean domain with norm given by the degree, and hence a PID and UFD. Moreover, the units are nonzero constant polynomials. Thus, each class of associates can be uniquely represented by a monic polynomial, i.e. one whose first coefficient is 1.

We also know that because $\mathbb{F}$ is a field, $(x - a)$ divides $f(x)$ iff $f(a) = 0$. Thus, we have

$$\mathbb{F}[x]/(x - a) \cong \mathbb{F}$$

where the isomorphism is given by $f \mapsto f(a)$.

Theorem 3.1 (**Fundamental Theorem of Algebra**). *In $\mathbb{C}[x]$, the only irreducible polyomials are linear.*

However, in $\mathbb{Q}[x]$, there are irreducible polynomials of arbitrarily large degree.

Proposition 3.3 (**Gauss' lemma**). *Let R be a UFD with field of fractions $\mathbb{F}$ and let $p(x) \in R[x]$. If $p(x)$ is reducible in $\mathbb{F}[x]$ then $p(x)$ is reducible in $R[x]$.*

Proposition 3.4. *Let R be a UFD and let $\mathbb{F}$ be its field of fractions. Consider any $p(x) \in R[x]$, such that the gcd of its coefficients is 1. Then $p(x)$ is irreducible in $R[x]$ iff it is irreducible in $\mathbb{F}[x]$.*

Theorem 3.2. *A ring R is a UFD iff the ring of polynomials $R[x]$ is a UFD.*

Proposition 3.5. *Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.*

Proposition 3.6 (**Eisenstein's Criterion**). *If R is an integral domain and $P \subseteq R$ is a maximal ideal, let $f(x) \in R[x]$ be a non-constant monic polynomial such that $a_i \in P$ for $0 \leq i \leq n - 1$ but $a_0 \notin P^2$. Then $f(x)$ is irreducible in $R[x]$.*

4 Introduction to Module Theory

Definition 4.1 (**Module**). *If R is a ring, a (left) R-module M is an abelian group (with addition) equipped with an action of R, i.e. a map $R \times M \to M$ where $(r, m) \mapsto rm$ satisfying*

- *$(r_1 r_2)m = r_1(r_2 m)$ for all $r_1, r_2 \in R$, $m \in M$*
- *$r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$, $m_1, m_2 \in M$*
- *$(r_1 + r_2)m = r_1 m + r_2 m$ for all $r_1, r_2 \in R$, $m \in M$*
- *If $1 \in R$, then $1(m) = m$ for all $m \in M$*

In other words, a module over a ring is analogous to a vector space over a field. For example, if $R = \mathbb{F}$ is a field, then an $\mathbb{F}$-module is just an $\mathbb{F}$-vector space V.

Example: For $R = \mathbb{Z}$, a $\mathbb{Z}$-module is just an abelian group.

Example: For $R = \mathbb{F}[x]$, an R-module is an $\mathbb{F}$-vector space V equipped with a linear operator $T : V \to V$ that gives the action of the variable x. Similarly, for $R = \mathbb{Z}[x]$, an R-module is an abelian group M with a homomorphism $T : M \to M$ that gives the action of the variable x.

Example: If $R = \mathbb{C}[x, y]/(y^2 - x^3)$, an R-module is a $\mathbb{C}$-vector space V equipped with linear maps $S, T : V \to V$ such that $S^2 = T^3$.

Definition 4.2 (**Submodules**). *If M is an R-module, an R-submodule of M is a subgroup $M' \leq M$ that is closed under the action of R. Thus, M' is itself an R-module.*

Proposition 4.1 (**Submodule criterion**). *Let R be a ring and let M be an R-module. A subset $N \subseteq M$ is a submodule if $N \neq \emptyset$ and for all $x, y \in N$ and $r \in R$, $x + ry \in N$.*

Example: If R is any ring, then the multiplication map $\times : R \times R \to R$ makes R an R-module. In this case, submodules of R are exactly (left) ideals.

Definition 4.3 (**Direct sum, product**). *Consider a collection of R-modules, $\{M_i\}_i$. We can define the direct product*

$$\prod_{i \in I} M_i$$

and give it the structure of an R-module by defining addition and the action componentwise. We can also define the direct sum

$$\bigoplus_{i \in I} M_i := \{(m_i) \in \prod M_i : m_i = 0 \text{ for all but finitely many } i\}$$

and still define addition and the action componentwise. Thus, in general,

$$\bigoplus_{i \in I} M_i \subseteq \prod_{i \in I} M_i$$

but the two are the same exactly when I is finite.

In particular, $\bigoplus_i R$ is the set of finite R-linear combinations of basis vectors e_i, which can be defined as long as $1 \in R$. In this case, we can meaningfully define the dimension of $M = \bigoplus_i R$ to be $|I|$. However, unlike in linear algebra, an R-module need not be a direct sum of copies of R - in these cases, it is not obvious how to define dimension.

Definition 4.4 (**Module homomorphism**). *If M, N are R-modules, a map $\varphi : M \to N$ is called a homomorphism if $\varphi : (M, +) \to (N, +)$ is a homomorphism of groups and $\varphi(rm) = r\varphi(m)$ for all $r \in R$, $m \in M$.*

Definition 4.5. *If $\varphi : M \to N$ is a homomorphism of R-modules, we define*

$$ker(\varphi) = \{m \in M : \varphi(m) = 0\} \subseteq M$$

In fact, $\ker(\varphi)$ is a submodule of M.

Definition 4.6 (**Quotient module**). *If M is an R-module and $M' \subseteq M$ is a submodule, then we can consider the quotient group M/M', and give it a module structure by defining the action as*

$$r(m + M') = (rm) + M'$$

for any $m \in M$.

Theorem 4.1 (**Isomorphism Theorems for Modules**). *We have the following theorems, analogous to the familiar statements.*

- *If $\varphi : M \to N$ is a module homomorphism then $M/\ker(\varphi) \cong \varphi(M)$.*
- *If A, B are submodules of the R-modules M, then $(A + B)/B \cong A(A \cap B)$.*
- *If M is an R-module with submodules A, B such that $A \subseteq B$, then $(M/A)/(B/A) \cong M/B$.*
- *If $M' \subseteq M$ is a submodule, then there is an inclusion-preserving bijection between submodules of M/M' and submodules of M containing M', given by the projection map.*

Now, given a fixed $m \in M$, an R-module, where $1 \in R$, we can define $\varphi : R \to M$ by $\varphi : r \mapsto rm$. Then φ is a module homomorphism where

$$\mathrm{Im}(\varphi) = \{rm : r \in R\}$$

is the submodule of M generated by m. In other words, it is a cyclic submodule. Then by the First Isomorphism Theorem,

$$\mathrm{Im}(\varphi) \cong R/\ker(\varphi)$$

where $\ker(\varphi) \subseteq R$ is a left ideal. Thus, cyclic modules have the form R/I for some ideal I.

Example: In the case $R = \mathbb{Z}$, we see that cyclic groups are of the form $\mathbb{Z}/(n)$, with finite order $|n|$ if $n \neq 0$ and isomorphic to $\mathbb{Z}$ if $n = 0$.

5 Classification of Finitely Generated Modules over a PID

Definition 5.1 (**Free module**). *An R-module M is called free if it has a basis $E \subseteq M$, i.e. every $m \in M$ can be uniquely represented as a (finite) R-linear combination of elements of E. If M is free, $|E| = n$ is called the rank.*

Definition 5.2 (**Rank**). *For any integral domain R, the rank of an R-module M is the maximum number of R-linearly independent elements of M.*

Specifically, to say that M is free of rank n is to say that it has a basis set of n elements. In this case, $M \cong R^{\oplus n}$.

Definition 5.3 (**Annihilator**). *Given an R-module M, it has a submodule called the annihilator defined by*

$$Ann(M) = \{r \in R : rm = 0 \ \forall m \in M\}$$

Definition 5.4 (**Finite generation**). *We say that an R-module M is finitely generated if there exist finitely many elements $m_1, m_2, \ldots, m_n \in M$ such that the M is generated by the m_i. In other words, any $v \in M$ has a representation as*

$$v = r_1 m_1 + \ldots + r_n m_n$$

for some coefficients $r_i \in R$.

Definition 5.5 (**Torsion**). *If M is a module over an integral domain R, an element $m \in M$ is called torsion if there exists $r \in R$ such that $r \neq 0$ but $rm = 0$.*

Definition 5.6 (**Torsion-free**). *If 0 is the only torsion element of a module M, it is called torsion-free.*

Example: An integral domain R is torsion-free as an R-module. More generally, so is $R^{\oplus n}$ for any $n \geq 1$.

Example: If $R = \mathbb{Z}$, then $\mathbb{Q}$ is torsion-free as a $\mathbb{Z}$-module. However, $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}^{\oplus d}$ for any d.

Lemma 5.1. *If M is an R-module, we can define the set of torsion elements, denoted by $Tor(M)$. Then $Tor(M) \subseteq M$ is a submodule.*

Lemma 5.2. *If M is finitely generated and torsion, then there exists $r \neq 0 \in R$ such that $rm = 0$ for all $m \in M$.*

Lemma 5.3. *If M is an R-module and $T \subseteq M$ is its torsion submodule, then M/T is torsion free as an R-module.*

Lemma 5.4. *If M is finitely-generated over a PID R and M is torsion-free then*

$$M \cong R^{\oplus d}$$

for some integer $0 \leq d < \infty$.

Lemma 5.5. *If M is finitely generated by $m_1, \ldots, m_n$ and $N \subseteq M$ is a submodule, then M/N is finitely generated by the cosets $[m_1], \ldots, [m_n]$.*

Theorem 5.6 (**Classification Theorem**). *If M is a finitely-generated module over a PID R, then M is a direct sum of finitely-many cyclic modules. Specifically, there exists $n \in \mathbb{N}_{\geq 0}$ and $T \subseteq M$, a finitely-generated torsion submodule, such that*

$$M \cong R^{\oplus n} \bigoplus T$$

Here, n is called the (free) rank of M, and the n copies of R are called the free part. Alternatively, there exist elements $a_1, a_2, \ldots, a_k \in R$ such that

$$M \cong R^{\oplus n} \oplus \bigoplus_{i=1}^{k} R/(a_i)$$

There are two canonical decompositions of M. First, it can be written as

$$M \cong R^{\oplus n} \oplus \bigoplus_{i=1}^{k} \bigoplus_{j} R/(p_j^{n_{ij}})$$

where the p_j are distinct primes, each $n_{ij} \geq 0$, and for all i,

$$a_i = \prod_{j=1}^{k(i)} p_j^{n_{ij}}$$

The terms $p_j^{n_{ij}}$ are called the elementary divisors. Alternatively, we can write

$$M \cong R^{\oplus n} \oplus R/(d_1) \oplus R/(d_2) \oplus \ldots \oplus R/(d_r)$$

where $d_1 | d_2 | \ldots | d_r$. The d_i are called invariant factors.

Theorem 5.7 (**Fundamental Theorem, Uniqueness**)**.** *Two finitely-generated R-modules M_1 and M_2 are isomorphic iff they have the same free rank and the same list of invariant factors, or the same list of elementary divisors.*

Corollary 5.7.1. *If A is a finitely-generated abelian group, then there exist $d_1, d_2, \ldots, d_r \in \mathbb{Z}$, $n \geq 0$, and powers of primes $p_j^{n_{i,j}}$ such that*

$$A \cong \mathbb{Z}^n \oplus (\mathbb{Z}/d_1\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/d_r\mathbb{Z}) \cong \mathbb{Z}^n \oplus \bigoplus_{i,j} \mathbb{Z}/p_j^{n_{i,j}}\mathbb{Z}$$

Corollary 5.7.2. *Let $\mathbb{F}$ be a field. Let $A \subseteq \mathbb{F}^\times$ be a finite subgroup. Then A is cyclic.*

Corollary 5.7.3. *For any prime p, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*