SUMMARY ALGEBRA I

LOUIS-PHILIPPE THIBAULT

Contents

1. Group Theory 1
1.1. Basic Notions 1
1.2. Isomorphism Theorems 2
1.3. Jordan- Holder Theorem 2
1.4. Symmetric Group 3
1.5. Group action on Sets 3
1.6. Sylow's theorems 4
1.7. Semidirect product 4
1.8. Some other useful facts 5
2. Ring Theory 5
2.1. Basic Notions 5
2.2. Isomorphism Theorems 6
2.3. Different types of Rings 6
3. Modules 8
3.1. Basic Notions 8
3.2. Direct Sum 9

1. Group Theory

1.1. Basic Notions.

Theorem 1.1. *$H \subset G$ is a subgroup iff $x, y \in H \Rightarrow xy^{-1} \in H$.*

Theorem 1.2. *If f is an isomorphism, then f^{-1} is an isomorphism.*

Theorem 1.3. *$N \leq G$ is normal $\Leftrightarrow gxg^{-1} \in N \ \forall \ x \in N, g \in G$.*

Definition 1.1 (Conjugaison). In Prof. Bar-Natan's notation, $x^g = g^{-1}xg$.
Automorphism = self-isomorphism, and the function defined by

$$x \to gxg^{-1}$$

is the Inner automorphism coming from g.

Theorem 1.4. *$Inn(G) \lhd Aut(G)$*

Theorem 1.5. *$Ker(\phi) \lhd G$*

Theorem 1.6. *Suppose $N \lhd G$. Then there exists a group H and an homomorphism $\phi : G \to H$ such that $N = Ker(\phi)$.*

Remark 1.1. Take $H = G/N$.

Definition 1.2 (Centralizer, normalizer, center). $X \subset G$.

- Centralizer: $C_G(X) = \{g \in G | gxg^{-1} = x \forall x \in X\}$.

- Centre: $Z(G) = C_G(G)$.
- Normalizer: $N_G(X) = \{g \in G | gXg^{-1} = X\}$.

Remark 1.2. If $X \leq G$, then X is a normal subgroup iff $N_G(X) = G$.

Theorem 1.7. *Let $< X >$ be the subgroup of G generated by X, i-e the smallest subgroup of G containing X. Then $C_G(X) = C_G(< X >)$ and $N_G(X) = N_G(< X >)$.*

1.2. **Isomorphism Theorems.**

Theorem 1.8 (Fundamental theorem of Homomorphisms)**.** *Let G, H be two groups and $\phi : G \to H$ be an homomorphism. Let $K \lhd G$ and $\psi : G \to G/K$ be the natural surjective homomorphism. If $K \subset Ker(\phi)$, then there exists a unique homomorphism $\alpha : G/K \to H$ such that $\phi = \alpha\psi$.*

Theorem 1.9 (First Isomorphism theorem)**.** *Let $\phi : G \to H$ be an homomorphism. Then $G/Ker(\phi) \cong Im(\phi)$.*

Theorem 1.10. *$H, K \leq G$. Then $HK \leq G \Leftrightarrow HK = KH$.*

Corollary 1.11. *Let H, K be subgroups of G. If $H \subset N_G(K)$, then $HK \leq G$ and $K \lhd HK$.*

Corollary 1.12. *If $K \lhd G$, then $HK < G$ for any $H \leq G$.*

Theorem 1.13 (Second Isomorphism Theorem)**.** *Let H, K be subgroups of G such that $H \subset N_G(K)$. Then, $(H \cap K) \lhd H, K \lhd HK$ and $HK/K \cong H/(H \cap K)$.*

Theorem 1.14 (Third Isomorphism Theorem)**.** *Let $K \lhd G$, $H \lhd G$, $K \leq H$. Then, $H/K \lhd G/K$ and $(G/K)/(H/K) \cong G/H$.*

Theorem 1.15. *Let $N \lhd G$. Then $q : G \to G/N$ induces a bijection between the subgroups of G which contain N and the subgroups of G/N.*

1.3. **Jordan- Holder Theorem.**

Theorem 1.16. *Givin a finite G, there exists a sequence $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 \triangleright \ldots \triangleright G_n = \{e\}$ such that $H_i = G_i/G_{i+1}$ is simple. Furthermore, the set $\{H_0, \ldots, H_{n-1}$ is unique up to a permutation.*

Remark 1.3. The sequence is called a tower and the set is called a composition series of G.

Definition 1.3 (solvable groups). A solvable group is a group whose Jordan-Holder composition series has only Abelian factors.

Definition 1.4 (commutator). Given $x, y \in G$, the commutator $[x, y]$ is given by $[x, y] = xyx^{-1}y^{-1}$. We denote by G' the group generated by all commutators of G.

Theorem 1.17. *$G' \lhd G$, G/G' is abelian and any morphism from G into an abelian group factors through G/G'.*

Remark 1.4. A equivalent definition of solvable groups is the following: A group G is solvable is there exists an n such that $G^{(n)} = \{e\}$, where $G^{(n)} = (G^{(n-1)})'$. The two definitions are equivalent because for every group G and every normal subgroup N of G, the quotient G/N is abelian $\Leftrightarrow$ N contains G'.

Example 1.1. A_n is not solvable for $n \geq 5$, because they are simple. In particular, $[A_n, A_n] = A_n$.

Theorem 1.18. *If $N \lhd G$, then G is solvable $\Leftrightarrow$ N and G/N are. Also, if $H < G$ and G is solvable, then H is solvable.*

1.4. **Symmetric Group.**

Theorem 1.19. *Let $\sigma, \tau \in S_n$, $\sigma = (a_1^{(1)} \dots a_1^{(r_1)}) \dots (a_n^{(1)} \dots a_n^{(r_n)})$. Then,*

$$\tau\sigma\tau^{-1} = (\tau^{-1}(a_1^{(1)}) \dots \tau^{-1}(a_1^{(r_1)})) \dots (\tau^{-1}(a_n^{(1)}) \dots \tau^{-1}(a_n^{(r_n)})).$$

Corollary 1.20. *$\tau\sigma\tau^{-1}$ have the same cycle decomposition as σ. Also, σ is conjugated to σ' if and only if σ and σ' have the same cycle type.*

Corollary 1.21. *The number of conjugacy classes in S_n is equal to the number of partitions of n.*

Theorem 1.22. *A_n is simple.*

Theorem 1.23. *S_4 contains no normal subgroup isomorphic to S_3.*

1.5. **Group action on Sets.**

Definition 1.5 (Group action). A group G acting on a set X is a binary map $G \times X \to X$, denoted $(g, x) \mapsto gx$ such that

- $(g_1, g_2)x = g_1(g_2x)$
- $ex = x$

Then X is called a G-set.

Definition 1.6 (Transitive set, Stabilizer, Orbits, fix points). Four definitions:

- Transitive set: X is transitive if for all $x, y \in X$, there exists $g \in G$ such that $gx = y$.
- Orbits: $Orb(x) = Gx = \{gx | g \in G\}$. X/G is the set of all orbits.
- Stabilizer: $Stab_X(x) = G_x = \{g \in G | gx = x\} < G$.
- Fix Points : $X^g = \{x \in X | gx = x\}$.

Definition 1.7 (G-morphisms). A map $f : X \to Y$ is a G-morphism between two G-sets if $f(gx) = gf(x)$ for all $g \in G$.

Theorem 1.24. *Three properties of group actions:*

- *Every G-set X is a disjoint union of transitive G-sets. Those are the orbits.*
- *If Y is a transitive G-set, then $Y \cong G/H$ as a G-set for some $H < G$.*
- *If X is a transitive G-set and $x \in X$, then $X \cong G/(Stab_X(x))$. So, $|X| \mid |G|$.*

Corollary 1.25. *If $|X| < \infty$ and x_i are representatives of the orbits, then*

$$|X| = \sum_i \frac{|G|}{|Stab_X(x_i)|} = \sum_i |G_{x_i}|.$$

Remark 1.5. In particular, $G/Stab_X(x_i) \cong G_{x_i}$, so $|G| = |Stab_X(x_i)| \cdot |G_{x_i}|$.

Theorem 1.26.

$$|Gx| = [G : G_x]$$

Theorem 1.27 (Burnside's lemma)**.**

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

where $|X/G|$ denotes the number of orbits.

Theorem 1.28. *If $|X| < \infty$ and x_i are the representatives of the orbits with more then one element, then*

$$|G| = |Z(G)| + \sum_i \frac{|G|}{|C_G(x_i)|}.$$

1.6. **Sylow's theorems.**

Definition 1.8 (Sylow-p subgroup). Let $|G| = p^\alpha m$, with $p \nmid m$. We say that $P < G$ is a Sylow-p subgroup of G if $|P| = p^\alpha$.

Lemma 1.29 (Cauchy Theorem)**.** *If A is an abelian group and $p \mid |A|$, then there exists some element of order p in A.*

Theorem 1.30 (Cauchy Theorem)**.** *If $p \mid |G|$, then there exists an element of order p in G.*

Theorem 1.31 (Sylow Theorem 1)**.** *Let $Syl_p(G) = \{P < G : |P| = p^\alpha\}$. Then $Syl_p(G) \neq \emptyset$.*

Theorem 1.32 (Sylow Theorem 2)**.** *Every p-subgroups of G is contained in some Sylow-p subgroup G.*

Two lemmas:

Lemma 1.33. *If $P \in Syl_p(G)$ and $H < N_G(P)$ is a p-group, then $H < P$.*

Lemma 1.34. *If $x \in G$ has order a power of p, and $x \in N_G(P)$, then $x \in P$.*

Theorem 1.35 (Sylow Theorem 3)**.** *Let $n_p(G) = |Syl_p(G)|$. Then,*

- *$n_p \mid |G|$;*
- *$n_p \equiv 1 \, mod \, p$;*
- *All Sylow-p subgroups of G are conjugate (so isomorphic) to each other.*

The Sylow-1 and Sylow-2 theorems can be deduced from the two following propositions.

Proposition 1.36. *If $R \in Syl_p(G)$, then $n_R(G) = |conjugates \ of \ R| \equiv 1 \, mod \, p$ and $n_R(G) \mid |G|$.*

Proposition 1.37. *If H is a p-subgroup of G and $P \in Syl_p(G)$, then H is contained in a conjugate of P.*

Example 1.2. See examples in the course notes of groups of order 12, 15, 21. Make sure that every n_p is possible. Sometimes not because of the lack of space. Also, make sure that every semi-direct product found is not isomorphic to another one. Also, if $P \lhd G$, then PQ is a subgroup. Then, if we now its order, and know how many $|Q|$-sylow subgroups it has, we can conclude that $Q \lhd PQ$ and so $|N_G(Q)| \geq |PQ|$. Then, it gives less room for the other Sylow subgroup. Also, if two elements x, y commute, then $|xy| = |x||y|$. The presentation will be of the form $\{\text{generator of } H \text{ and } N | \text{presentation of } N, \text{presentation of } H, yxy^{-1} = \phi_y(x)\}$.

1.7. **Semidirect product.**

Theorem 1.38. *If $K \lhd G$, $H \lhd G$, $K \cap H = \{e\}$, then $KH \cong K \times H$.*

Definition 1.9 (Semidirect product). Suppose N, H are groups and $\phi : H \to Aut(N)$ is a homomorphism. Then the semi-direct product of N and H is defined as follow:

$$N \rtimes_\phi H = N \times H$$

with product

$$(n_1, h_1)(n_2, h_2) \equiv (n_1 \phi(n_2), h_1 h_2)$$

Theorem 1.39. *$G = N \rtimes H$ is a group. Also, $H < G$, $N \lhd G$, $G/N = H$, $G = NH$.*

Theorem 1.40. *If $G = NH$, $N \lhd G$, $H < G$, $H \cap N = \{e\}$. Then, $G \cong N \rtimes_\phi H$, where $\phi_h(n) = hnh^{-1}$.*

Theorem 1.41. *Let $\phi : G \to K$ be a group homomorphism. Suppose there exists a group homomorphism $s : K \to G$ such that $\phi s = 1_K$. Then,*

$$G \cong Ker(\phi) \rtimes K.$$

Theorem 1.42. *Let $H \lhd G$. Let $i : H \to G$ be the inclusion map. Suppose there exists a group homomorphism such that $ri = 1_H$. Then,*

$$G \cong H \times G/H.$$

1.8. **Some other useful facts.**

Theorem 1.43. *Let G be a group. Then, $\phi : G \to G$ given by $\phi(g) = g^2$ is a homomorphism if and only if G is abelian.*

Theorem 1.44. *If $G/Z(G)$ is cyclic, then G is abelian. Moreover, if $Aut(G)$ is cyclic, then G is abelian.*

Theorem 1.45. *Let G be a group, and H be a subgroup of finite index. Then there exists a normal subgroup N of G such that N is contained in H and $[G : N] < \infty$.*

Theorem 1.46. *$Aut(\mathbb{Z}_p) = C_{p-1}$.*

2. Ring Theory

2.1. **Basic Notions.**

Definition 2.1 (Ring). A ring is a set R with two binary operations:

$$+ : R \times R \to R$$

$$\cdot : R \times R \to R$$

and two elements $0 \neq 1 \in R$ (1 is not always required) such that

(1) (R,+,0) is an Abelian group;
(2) For all a, b, c $(ab)c = a(bc)$;
(3) $1 \cdot a = a \cdot 1 = a$, $\forall a$;
(4)
- $(a + b)c = ac + bc$;
- $a(b + c) = ab + ac$.

Example 2.1. Given a ring R, we can define the **polynomial ring with coefficients in** R, denoted by $R[x]$. $R[x] = \{\sum_{i=0}^{d} \alpha_i x^i | \alpha_i \in R\}$. The multiplication is given by:

$$(\sum_{i=0}^{d_1} a_i x^i)(\sum_{i=0}^{d_2} b_j x^j) = \sum_{k=0}^{d_1+d_2} (\sum_{i=0}^{k} a_i b_{k-i}) x^k).$$

Definition 2.1 (Ring homomorphism). If R, S are rings, a **ring homomorphism** $\phi : R \to S$ has the following properties:

(1) $\phi(0) = 0, \phi(1) = 1$;
(2) $\phi(a + b) = \phi(a) + \phi(b)$;
(3) $\phi(ab) = \phi(a)\phi(b)$.

Definition 2.2 (Kernel). The **Kernel** of an homomorphism is given by $Ker(\phi) = \phi^{-1}(0)$.

Definition 2.3 (Ideal). $I \subset R$ is called an **ideal** if it is an additive subgroup of R and if $r \in R$, $a \in I$ implies $ra, ar \in I$.

Theorem 2.1. *Given R, S two rings and $\phi : R \to S$ a morphism, we have*

(1) *$Im(\phi)$ is a subgroup of S.*
(2) *$Ker(\phi)$ is not a subring because it does not contain* 1*. In fact, it is an ideal in R.*

As in group theory, given $I \subset R$ an ideal in a ring, there is always a morphism $\phi : R \to S$ such that $Ker(\phi) = I$. In fact, just take the quotient ring $S = R/I$. s

Definition 2.4 (Quotient ring). Define an equivalence relation $\sim$ on R by $r_1 \sim r_2$ if $r_1 - r_2 \in I$, then the quotient ring is

$$S = R/\sim = R/I = \{[r]_I | r \in R\}.$$

It is a ring.

Definition 2.5 (Ideal generated by $A \subset R$). The ideal generated by A, denoted by $\langle A \rangle$, is the smallest ideal containing A. It is also the intersection of all ideals containing A.

Theorem 2.2.

$$\langle A \rangle = \{\sum_{i=1}^{n} r_i a_i r_i' | a_i \in A, r_i, r_i' \in R\}.$$

2.2. **Isomorphism Theorems.** The isomorphism theorems are analogous to those in group theory. The proofs are similar.

Theorem 2.3 (First Isomorphism theorem)**.** *Given $\phi : R \to S$ a ring homomorphism. Then*

$$R/Ker\phi \cong Im\phi.$$

Example 2.2. $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a ring isomorphic to $\mathbb{C}$, using the first isomorphism theorem.

Theorem 2.4 (Second Isomorphism theorem)**.** *Given $A \subset R$ a subring and $I \subset R$ an ideal, we have*

$$(A + I)/I \cong A/(A \cap I).$$

Theorem 2.5 (Third Isomorphism theorem)**.** *If $I \subset J \subset R$ are both ideals, then*

$$(R/I)/(J/I) \cong R/J.$$

Theorem 2.6 (Fourth Isomorphism Theorem)**.** *If I is an ideal in R, then there is a bijection between ideals in R/I and ideals between I and R.*

2.3. **Different types of Rings.**

Definition 2.6 (Field). If R is commutative and R^* is a group, then we say that R is a **field**.

Definition 2.7 (Division Ring). If R^* is a group, then we say that R is a **division ring**.

Example 2.3. The Quaternions, denoted by $\mathbb{H}$, are a non-commutative division ring:

$$\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j\}.$$

We will now always assume without saying it that R is **commutative** unless otherwise explicitly stated.

Definition 2.8 (Integral domain). R is an **integral domain** if whenever $a \neq 0$,

$$ab = 0 \Rightarrow b = 0.$$

Remark 2.1. R is an integral domain if and only if whenever $a \neq 0$,

$$ab = ac \Rightarrow b = c.$$

Definition 2.9 (0 divisors). If $a \neq 0$, and there exists $b \neq 0$ such that $ab = 0$, then we say that a is a **0 divisor**. It is clear that R is an integral domain if and only if it is abelian and it has no 0-divisor.

Definition 2.10 (Maximal Ideals). An ideal $I \subset R$ is **maximal** if

(1) $I \neq R$ ($1 \notin I$);
(2) If $J \supset I$ is an ideal, then $J = I$ or $J = R$.

Lemma 2.7. *A field F is a ring whose only ideals are $\{0\}$ and F.*

Theorem 2.8. *Given a ring R and an ideal I, R/I is a field if and only if I is maximal.*

Theorem 2.9. *Every ideal is contained in a maximal ideal.*

Definition 2.11 (Prime ideal). An ideal $P \subset R$ is called **prime** if whenever $b \notin P$, $ab \in P \Rightarrow a \in P$.

Theorem 2.10. *$P \subset R$ is prime if and only if R/P is a domain.*

Corollary 2.11. *Every maximal ideal is prime.*

Example 2.4. A example of a prime ideal not maximal is $\langle x \rangle \subset \mathbb{Z}[x]$. Indeed, $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ is a domain, but not a field.

We now assume R is a **domain**.

Definition 2.12 (Division). Let $a, b \in R$. We say that a divides b and write $a|b$ if there exists c such that $ac = b$.

Theorem 2.12. *If $a|b$ and $b|a$, then $a = ub$, where u is a **unit**, that is, u is invertible.*

Remark 2.2. In this case, we say that $a \sim b$. This is an equivalence relation.

Definition 2.13 (Greatest Common Divisor). Given $a, b \in R$, we say that q is a **greatest common divisor** of a and b if

(1) $q|a$ and $q|b$;
(2) If $q'|a$ and $q'|b$, then $q'|q$.

Remark 2.3. There exists not always a g.c.d., but if one exists, it is unique up to a unit.

Definition 2.14 (Prime). If $p \in R \setminus (R^* \cup \{0\})$, then we say that p is a **prime** if $p|ab \Rightarrow p|a$ or $p|b$.

Remark 2.4. It follows that such p is prime if and only if $\langle p \rangle$ is prime.

Definition 2.15 (Irreducible). If $x \in R \setminus (R^* \cup \{0\})$, then we say that x is **irreducible** if $x = ab \Rightarrow a \in R^*$ or $b \in R^*$.

Remark 2.5. Every prime is irreducible. However, the converse is not true.

Example 2.5. In $\mathbb{Z}[\sqrt{-5}]$, 2 is irreducible but not a prime.

Definition 2.16 (Unique Factorisation domain). A ring R is a **unique factorization domain** if every non-zero element in R can be factored as a product of primes, i.-e., if $x \neq 0$, then there exists primes $p_1, p_2, \ldots, p_n$ such that $x = up_1, p_2, \ldots, p_n$, where $u \in R^*$.

Theorem 2.13. *Such a decomposition is unique up to units and permutations.*

Theorem 2.14. *In a UFD R, an element $x \in R$ is prime if and only if it is irreducible.*

Theorem 2.15. *A ring R is a UFD if and only if every nonzero element of R has a unique decomposition into irreducible elements.*

Theorem 2.16. *In a UFD, $gcd(a, b)$ always exists.*

Definition 2.17 (Euclidean domain). A ring R is a **Euclidean domain** if it has an **Euclidean norm**:

$$e : R \setminus \{0\} \to \mathbb{N},$$

such that

(1) $e(ab) \geq e(a)$ for all $b \in R$;
(2) For all $a, b \in R \setminus \{0\}$, there exists $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $e(r) < e(b)$.

Example 2.6. Two examples:

(1) $\mathbb{Z}$ with $e(a) = |a|$ is a Euclidean domain.
(2) Let $\mathbb{F}$ be a field. Then $R = \mathbb{F}[x]$ is Euclidean with $e(f) = deg(f)$.

Definition 2.18 (Principal Ideal domain). R is a **principal ideal domain** if every ideal in R is **principal**, that is, generated by a single element.

Theorem 2.17. *Every Euclidean domain is a principal ideal domain.*

Theorem 2.18. *In a PID, every prime ideal is maximal.*

Definition 2.19 (Noetherian ring). A **Noetherian ring** is a ring in which whenever $I_1 \subset I_2 \subset I_3 \subset \ldots$ is an increasing chain of ideals, then there exists N such that $n \geq N \Rightarrow I_n = I_{n+1}$.

Lemma 2.19. *Every PID is Noetherian.*

Theorem 2.20. *Every PID is a UFD.*

Remark 2.6. In a PID, $\langle a, b\rangle = \langle gcd(a, b)\rangle$. In particular, there exists $s, t \in R$ such that $gcd(a, b) = sa + tb$.

Remark 2.7. In a Euclidean domain, the Euclidean algorithm is a pratical way to find s and t in remark 2.6.

Remark 2.8. A ring R is a PID if and only if it has a **Dedekind-Hasse norm**

$$d : R \setminus \{0\} \to \mathbb{N} \setminus \{0\},$$

such that if $a, b \neq 0$, then either $a \in \langle b\rangle$ or there exists $0 \neq x \in \langle a, b\rangle$ such that $d(x) < d(b)$.

3. Modules

3.1. Basic Notions.

Definition 3.1 (R-modules). Let M be an Abelian group and R be a ring. Then M is an **left R-module** if there exists a map $R \times M \to M$, $(r, m) \mapsto rm$ such that

(1) $1 \cdot m = m$;
(2) $a(bm) = (ab)m$;
(3) $(a + b)m = am + bm$, $a(m_1 + m_2) = am_1 + am_2$.

A **right R-module** is defined similarly.

Example 3.1. The following are R-modules:

- Vector space over a field;
- Any abelian group A is a module over $\mathbb{Z}$;
- If V is a vector space over $\mathbb{F}$, $T : V \to V$ a linear map, then V is a $\mathbb{F}[x]$-module, by
$$(\sum a_i x^i)v = \sum a_i T^i(v).$$
- If I is an ideal in R, then I and R/I are R-modules.
- If $R = M_{n\times n}(S)$, then S^n is a left R-module and $(S^n)^T$ is a right R-module.

Definition 3.2 (Homomorphism of R-modules). Let M, N be R-modules. Then a map $\phi : M \to N$ is a **homomorphism of R-modules** if it is a group homomorphism and

$$r\phi(m) = \phi(rm).$$

Theorem 3.1. *If $A \subset M$ is a R-submodule, then M/A is an R-module.*

Remark 3.1. $ker(\phi), Im(\phi)$ are submodules and the four isomorphism theorems hold.

3.2. **Direct Sum.**

Definition 3.3 (Direct Sum (def 1)). Let M, N be R-modules. Then, $M \oplus N = \{(m, n) | m \in M, n \in N\}$ is called the **direct sum** of M and N. The scalar product is defined as follow: $r(m, n) = (rm, rn)$.

Definition 3.4 (Direct Sum (def 2)). Let M, N be R-modules. The **direct sum** of M and N, denoted $M \oplus N$, is a R-module having the following property:
Let $\phi_M : M \to M \oplus N$ and $\phi_N : N \to M \oplus N$. If there exists a R-module P such that there exists morphisms $\psi_M : M \to P$ and $\psi_N : N \to P$, then there exists a unique morphism $\alpha : M \oplus N \to P$ such that $\psi_M = \alpha\phi_M$ and $\psi_N = \alpha\phi_N$. Such a module exists and is unique.

Definition 3.5 (Direct Product). Let M, N be R-modules. The **direct product** of M and N, denoted $M \oplus N$, is a R-module having the following property:
Let $\phi_M : M \oplus N \to M$ and $\phi_N : M \oplus N \to N$. If there exists a R-module P such that there exists morphisms $\psi_M : P \to M$ and $\psi_N : P \to N$, then there exists a unique morphism $\alpha : P \to M \oplus N$ such that $\psi_M = \phi_M\alpha$ and $\psi_N = \phi_N\alpha$. Such a module exists and is unique.

Theorem 3.2. *The definitions of finite direct product and finite direct sum are equivalent.*