Representation theory

Gabriele Dalla Torre
gabrieledallatorre@gmail.com

November 12, 2010

Notes for lectures given by Prof. Hans Cuypers and Prof. Hendrik W. Lenstra at Vrije Universiteit (Free University) Amsterdam, Fall 2010

Contents

1 Historical and mathematical background **1**

2 Solvable groups **3**

3 Modules **6**

4 Modules and representation theory **10**

5 Exact sequences **13**

6 Homomorphisms and tensors **15**

7 Jordan-Hölder Theorem and Grothendieck groups **26**

8 Additive invariants **33**

9 Semisimplicity **41**

10 Traces and characters **50**

11 Integrality and Burnside's theorem **57**

12 The restriction map and Frobenius' theorem **63**

13 Computing the character table **69**

14 Induction and Brauer's theorem **72**

Chapter 1

Historical and mathematical background

Let G be a finite group and k be a field. We shall often have $k = \mathbb{C}$, but we actually need only that k is an algebraic closed field of characteristic 0.

Definition 1.1 (Representation)**.** A *representation* of a group G over a field k is a finite dimensional k-vector space V together with a group homomorphism

$$\rho : G \longrightarrow \mathrm{Aut}_k\, V.$$

The *dimension* of the representation is the dimension of V.

We denote by $\mathrm{M}(n, k)$ the ring of n-by-n matrices with entries from k. It is known that $\mathrm{GL}(n, k) = \{A \in \mathrm{M}(n, k) : \det A \in k^*\} = \mathrm{M}(n, k)^*$.

The matrix ring $\mathrm{M}(0, k)$ has one element: (), with determinant 1. Therefore $\mathrm{GL}(0, k) = \mathrm{M}(0, k)^* = \{()\}$ and the unique representation of dimension 0 is the trivial homomorphism. We also know that $\mathrm{GL}(1, k) = k^*$. This is an abelian group. If the dimension is greater than 1, then for every field k the group $\mathrm{GL}(n, k)$ is non-abelian.

Definition 1.2 (Equivalent representations)**.** Two representations $\rho, \rho' : G \longrightarrow \mathrm{GL}(n, k)$ are *equivalent representations* if there exists an $A \in \mathrm{GL}(n, k)$ such that for all $\sigma \in G$

$$\rho'(\sigma) = A\rho(\sigma)A^{-1}.$$

Later we shall give another definition of representation: A representation of a group G on a field k is a $k[G]$-module of finite k-dimension.

Two pioneers of representation theory are Dedekind (1831–1916) and Frobenius (1849–1917). Dedekind was interested in studying normal bases of number fields and that led him to introduce the concept of group determinant.

Definition 1.3 (Group determinant)**.** Let G be a finite group. The *group determinant* of G is

$$\det\left[X_{\sigma\tau^{-1}}\right]_{\sigma,\tau\in G} \in \mathbb{C}[X_\sigma : \sigma \in G].$$

Examples. If G is a group order 2, then the group determinant factors in the following way:

$$\begin{vmatrix} X_1 & X_2 \\ X_2 & X_1 \end{vmatrix} = X_1^2 - X_2^2 = (X_1 + X_2)(X_1 - X_2).$$

If G is a group of order 3, then we have

$$\begin{vmatrix} X_1 & X_3 & X_2 \\ X_2 & X_1 & X_3 \\ X_3 & X_2 & X_1 \end{vmatrix} = (X_1 + X_2 + X_3)(X_1 + \zeta X_2 + \zeta^2 X_3)(X_1 + \zeta^2 X_2 + \zeta X_3),$$

where $\zeta = e^{\frac{2\pi i}{3}}$ is a primitive third root of unity.

Dedekind found the following expression for the group determinant of a finite abelian group G:

$$\det\left[X_{\sigma\tau^{-1}}\right]_{\sigma,\tau\in G} = \prod_{\rho}\sum_{\sigma\in G}\rho(\sigma)X_\sigma,$$

where ρ runs over all group homomorphisms $\rho : G \longrightarrow \mathrm{GL}(1,\mathbb{C}) = \mathbb{C}^*$. The number of these group homomorphisms is equal to the order of G.

If G is a finite group, then we call $\mathrm{Hom}(G,\mathbb{C}^*) = \hat{G}$ the *dual group* of G. If G is an abelian finite group, then $\#\hat{G} = \#G$. There exists a canonical isomorphism between $\hat{\hat{G}}$ and G.

In a letter to Frobenius, dated 25 March 1896, Dedekind posed the problem of factoring the group determinant of a finite non-abelian group into irreducible factors. Frobenius solved the problem and published the solution in the same year.

The group determinant of the group S_3 is the product of two irreducible polynomials of degree 1 and the square of an irreducible polynomial of degree 2. What is the general theory?

Let G be a finite group of order n. Then

$$\det\left[X_{\sigma\tau^{-1}}\right]_{\sigma,\tau\in G} = \prod_{i=1}^{t} P_i^{n_i},$$

with $P_i \in \mathbb{C}[X_\sigma : \sigma \in G]$ irreducible, homogeneous polynomials of degree n_i and pairwise distinct.

By comparing degrees, we get

$$n_1^2 + n_2^2 + n_3^2 + \ldots + n_t^2 = n.$$

It is also true that t is equal to the number of conjugacy classes of G. Moreover, for all $i = 1,\ldots,t$ we have that n_i is a divisor of n and the number of linear factors in the group determinant is equal to the index of the commutator subgroup of G in G. We shall denote the commutator subgroup of G by $[G,G]$.

Examples. Let Q be the quaternion group. It has order 8 and we denote its elements by $\pm 1, \pm i, \pm j, \pm k$. There are 5 conjugacy classes: $\{1\}$, $\{-1\}$, $\{\pm i\}$, $\{\pm j\}$, and $\{\pm k\}$. Since the commutator subgroup $[Q,Q]$ is equal to $\langle -1\rangle$, the number of linear factors in the group determinant is $8/2 = 4$. Hence, $8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2$.

If G is S_4, then $n = 24$ and $t = 5$. Moreover, the commutator subgroup is A_4. Hence, $24 = 1^2 + 1^2 + 2^2 + 3^2 + 3^2$.

In the general case the solution by Frobenius is

$$\det\left[X_{\sigma\tau^{-1}}\right]_{\sigma,\tau\in G} = \prod_{\rho}\left(\det\left(\sum_{\sigma\in G}\rho(\sigma)X_\sigma\right)\right)^{\dim\rho},$$

where ρ runs over all irreducible representations of G up to equivalence. We shall give later the definition of irreducible representation.

Note that $\rho(\sigma)$ is an element of $\mathrm{GL}(n,\mathbb{C})$. Therefore $\sum_{\sigma\in G}\rho(\sigma)X_\sigma$ is an element of $\mathrm{M}(\dim\rho, \mathbb{C}[X_\sigma : \sigma \in G])$.

Chapter 2

Solvable groups

Now we are going to formulate a theorem of group theory which can be proven by using representation theory. Before stating it, we need some definitions and theorems.

Definition 2.1 (Solvable group)**.** A group G is *solvable* if there exists a chain of subgroups

$$\{\mathrm{id}\} = G_0 \subset G_1 \subset \ldots \subset G_{t-1} \subset G_t = G$$

with $t \in \mathbb{Z}_{\geq 0}$ such that for every $0 < i \leq t$ the group G_{i-1} is normal in G_i and G_i/G_{i-1} is abelian.

The condition that G_{i-1} is normal in G_i and G_i/G_{i-1} is abelian is equivalent to the condition that $G_i \supset G_{i-1} \supset [G_i, G_i]$.

Example. The permutation group S_4 is solvable: $\{\mathrm{id}\} \subset V_4 \subset A_4 \subset S_4$. Note that this chain is not unique, because it can be refined to $\{\mathrm{id}\} \subset \langle(1\ 2)(3\ 4)\rangle \subset V_4 \subset A_4 \subset S_4$.

Using the following procedure we can determine whether a group G is solvable and, if so, we can simultaneously construct a chain of subgroups. A group G is solvable if and only if the chain

$$G = G_t \supset G_{t-1} = [G_t, G_t] \supset G_{t-2} = [G_{t-1}, G_{t-1}] \supset \ldots$$

reaches the trivial group in a finite number of steps. In this way we always find a chain of subgroups such that for every $0 < i \leq t$ the group G_{i-1} is normal in G and not only in G_i.

Example. The permutation group S_5 is not solvable: $S_5 \supset [S_5, S_5] = A_5 = [A_5, A_5]$.

When G is a finite solvable group, we can always construct a chain such that the quotients G_i/G_{i-1} are not only abelian, but even cyclic. In some cases we do not have any more that all subgroups of the chain are normal in G. Actually, the existence of a chain

$$G = G_t \supset G_{t-1} \supset \ldots \supset G_1 \supset G_0 = \{\mathrm{id}\}$$

such that for every $0 < i \leq t$ the quotients G_i/G_{i-1} are cyclic and the subgroup G_{i-1} is normal in G is a stronger statement than requiring G to be solvable.

We can immediately see that some groups are solvable.

Definition 2.2 (p-group)**.** Let p be a prime number. A torsion group G is a *p-group* if each element of G has a power of p as its order.

Theorem 2.3. *Let p be a prime number and G be a finite p-group. Then G is solvable.*

Definition 2.4 (p-Sylow subgroup)**.** Let p be a prime number and G be a finite group. Let p^k be the largest power of p dividing the order of G. Any subgroup of G of order p^k is called *p-Sylow subgroup.*

Theorem 2.5. *Let p be a prime number and G be a finite group. Then G contains a p-Sylow subgroup and all p-Sylow subgroups of G are conjugate.*

Theorem 2.6 (Burnside (1904))**.** *Let G be a group of order $p^a q^b$ where p and q are prime numbers and a, $b \in \mathbb{Z}_{\geq 0}$. Then G is solvable.*

We shall use representation theory in order to prove this theorem. There is also a proof which does not use it.

A strong result is the following theorem, which is known as Odd Order Theorem. We shall not give a proof, because is too long to be presented in this course.

Theorem 2.7 (Feit, Thompson (1963))**.** *Every finite group of odd order is solvable.*

As a reference you can see the book [1] by Bender and Glauberman and the book [2] by Peterfalvi.

A concept related to solvable groups is the notion of simple group.

Definition 2.8 (Simple group)**.** A *simple group* is a nontrivial group whose normal subgroups are only the trivial group and the group itself.

For example, the alternating groups A_n for $n \geq 5$ are simple. All finite simple groups have been classified and the proof consists of several thousands of pages written by about one hundred mathematicians.

If a group G is not simple, then it has a normal subgroup N with $N \neq G$ and $N \neq \{\mathrm{id}\}$. A strategy which can be used to prove that G is solvable is an argument by induction based on the assumption that both N and G/N are solvable.

The following theorem gives an explicit way to find a nontrivial normal proper subgroup for some groups. It is known only one proof of this theorem and it uses representation theory.

Theorem 2.9. *Let G be a finite group and let $C \subset G$ be a conjugacy class such that $\#C = p^n$ with p prime and $n \geq 1$. Then the subgroup of G generated by $\{\sigma\tau^{-1} : \sigma, \tau \in C\}$ is a normal subgroup of G different from $\{\mathrm{id}\}$ and G.*

Example. Let S_3 be the symmetric group on the set $\{1, 2, 3\}$, that is

$$S_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

The conjugacy classes of S_3 are $C_1 = \{\mathrm{id}\}$, $C_2 = \{(1\ 2), (1\ 3), (2\ 3)\}$ and $C_3 = \{(1\ 2\ 3), (1\ 3\ 2)\}$. Both C_2 and C_3 have prime power order and thus they meet the conditions of the theorem. Both conjugacy classes give the same normal subgroup, namely $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. This is A_3, the only normal subgroup of S_3 besides $\{\mathrm{id}\}$ and S_3.

We shall use Theorem 2.9 in the proof of Burnside's theorem. In order to prove Burnside's theorem we need some notions of representation theory.

Theorem 2.10. *Let G be a group and $N \lhd G$ be a normal subgroup. Then G is solvable if and only if both N and G/N are solvable.*

Definition 2.11 (Center)**.** Let G be a group. The *center* $Z(G)$ of G is the set of elements of G which commute with every element of G.

Note that $Z(G)$ is a normal subgroup of G and any subgroup of $Z(G)$ is normal in G.

Theorem 2.12. *Let G be a nontrivial group of prime power order. Then $\#Z(G) > 1$.*

Theorem 2.13. *Every group of prime power order is solvable.*

Note that this follows by induction on the order of the group from the previous facts. Indeed, $Z(G)$ is a normal subgroup of G different from $\{\mathrm{id}\}$. We may suppose that $Z(G) \neq G$, otherwise G is abelian and hence solvable. By inductive hypothesis $Z(G)$ and $G/Z(G)$ are solvable. Therefore, G is also solvable.

Definition 2.14 (Normalizer)**.** Let G be a group and τ be an element of G. The *normalizer* $N_G(\tau)$ of τ in G is the set of elements of G which commute with τ.

Let $C = \{\sigma\tau\sigma^{-1} : \sigma \in G\}$ be the conjugacy class of τ. Then $\#C = [G : N_G(\tau)]$, the index of $N_G(\tau)$ in G.

Proof of Burnside's theorem. Let G be a finite group of order $p^a q^b$ with p, q prime numbers and $a, b \in \mathbb{Z}_{\geq 0}$. We shall use induction on the order of G.

If G has prime power order, then it is solvable by Theorem 2.13. Therefore, we may assume that $\#G = p^a q^b$ with $p \neq q$, $a \geq 1$, $b \geq 1$. We want to construct a normal subgroup $N \lhd G$ such that $N \neq \{\mathrm{id}\}$, $N \neq G$.

Let $H \subset G$ be a q-Sylow subgroup. Hence, $\#H = q^b$. By Theorem 2.13 we can choose $\tau \in Z(H)$, $\tau \neq \mathrm{id}$. The element τ commutes with all elements of H and thus $H \subset N_G(\tau)$. This implies that $[G : N_G(\tau)] \mid [G : H] = p^a$ and we get $[G : N_G(\tau)] = p^n$ with $0 \leq n \leq a$.

If $n = 0$, then $N_G(\tau) = G$, that is for all $\sigma \in G$ we have $\sigma\tau\sigma^{-1} = \tau$. Hence, $\langle\tau\rangle$ is a normal nontrivial subgroup of G. We take $N = \langle\tau\rangle$, because $N \neq \{\mathrm{id}\}$. Either $N = G$, that is G is cyclic and therefore solvable, or $N \neq G$ and we are done.

Now suppose $n \geq 1$ and let C be conjugacy class of τ. Then $\#C = [G : N_G(\tau)] = p^n$ and Theorem 2.9 gives the requested N.

Both groups N and G/N have order less than $\#G$. Since the product of their orders is $p^a q^b$, then both $\#N$ and $\#G/N$ are products of two prime powers. By inductive hypothesis N and G/N are solvable. Hence, G is also solvable. □

The following theorem gives a way to construct a normal subgroup.

Theorem 2.15 (Frobenius (1901))**.** *Let G be a group which acts transitively on a finite set X and for all $\sigma \in G$ denote by n_σ the cardinality of the set $\{x \in X : \sigma x = x\}$. If for all $\sigma \in G \backslash \{1\}$ it holds that $n_\sigma \leq 1$, then $\{1\} \cup \{\sigma \in G : n_\sigma = 0\}$ is a normal subgroup of G which acts transitively on X.*

Examples. Let $G = S_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$ acts on the set $X = \{1, 2, 3\}$. We see that $n_\sigma = 3$ if $\sigma = \mathrm{id}$, $n_\sigma = 0$ if σ is a 3-cycle, and $n_\sigma = 1$ if σ is a 2-cycle. Theorem 2.15 states that $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$ is a normal subgroup of S_3. This group is again A_3.

Let D_5 be the dihedral group acting on the five vertices of a regular pentagon. Thus $n_\sigma = 5$ if σ is the identity, $n_\sigma = 0$ if σ is a nontrivial rotation, and $n_\sigma = 1$ if σ is a reflection. By Theorem 2.15 we get that the group of rotations is a normal subgroup of D_5.

Let $X = k$ be a finite field of order q. We define the group G by

$$G = \{\sigma : k \to k : \exists a_\sigma \in k^*, b_\sigma \in k : \forall x \in k : \sigma(x) = a_\sigma x + b_\sigma\}.$$

The order of G is $q(q-1)$. An element $\sigma \in G$ fixes exactly one point of X if the associated a_σ is equal to 1, namely the point $x = -b_\sigma(a_\sigma - 1)^{-1}$. If $a_\sigma = 1$ and $b_\sigma = 0$, then σ is the identity and fixes all points of X. If $a_\sigma = 1$ and $b_\sigma \neq 0$, then σ fixes no points. Theorem 2.15 says that the set $\{\sigma : \sigma \in G, a_\sigma = 1\}$ is a normal subgroup of G.

Chapter 3

Modules

We only consider rings with identity.

Definition 3.1 (Left R-module)**.** Let R be a ring. A *left R-module* is an abelian group M with a map $R \times M \to M$, $(r, m) \mapsto rm$ such that for all $r, s \in R$ and $m, n \in M$

$$\begin{aligned} r(m+n) &= rm + rn, \\ (r+s)m &= rm + sm, \\ (rs)m &= r(sm), \\ 1m &= m. \end{aligned}$$

It is not strictly necessary to require that the underlying group is abelian, because it follows from the properties of the map in the definition. The relations $r0 = 0$, $0m = 0$ and $-1m = -m$ can be also deduced from some properties.

An equivalent definition is the following. Let R be a ring. A *left R-module* is an abelian group M together with a ring homomorphism $\varphi : R \to \mathrm{End}(M)$. From this definition we immediately see that, given two rings R_1 and R_2, a ring homomorphism $f : R_1 \to R_2$, and an R_2-module M with $\varphi : R_2 \to \mathrm{End}(M)$, the group M with the ring homomorphism $\varphi \circ f : R_1 \to \mathrm{End}(M)$ is an R_1-module.

When we consider the underlying abelian group as a multiplicative group, we write the element rm as m^r or ${}^r m$. Note that in this case the property $(rs)m = r(sm)$ has the anti-intuitive form $m^{(rs)} = (m^s)^r$.

Besides left R-modules, which we shall shortly call R-modules, there are also *right R-modules*.

The ring R^{opp} has the same underlying additive group of R, whereas the multiplication is given by $r \cdot_{\mathrm{opp}} s = s \cdot r$. An *antihomomorphism* between two rings is a ring homomorphism where $f(rs) = f(s)f(r)$ instead of $f(rs) = f(r)f(s)$.

Definition 3.2 (Right R-module)**.** Let R be a ring. A *right R-module* is an abelian group M together with a ring homomorphism $\varphi : R^{\mathrm{opp}} \to \mathrm{End}(M)$ or, equivalently, an antihomomorphism $\varphi : R \to \mathrm{End}(M)$.

Definition 3.3 (Bimodule)**.** Let R and S be rings. An *R-S-bimodule* is an abelian group M which is a left R-module and a right S-module such that for all $r \in R$, $s \in S$, $m \in M$ it holds that $r(ms) = (rm)s$.

Homomorphisms of R-modules are defined as follows.

Definition 3.4 (R-homomorphism)**.** Let R be a ring and let M and N be two R-modules. An *R-homomorphism* or *R-linear map* from M to N is a group homomorphism $f : M \to N$ such that for all $r \in R$, $x \in M$ it holds that $f(rx) = rf(x)$.

Definition 3.5 (Isomorphism)**.** Let $f : M \to N$ be an R-linear map. The map f is an *isomorphism* of R-modules if there exists an R-linear map $g : N \to M$ such that $f \circ g = \mathrm{id}_N$ and $g \circ f = \mathrm{id}_M$.

Similarly to the case of rings, we may define the following sets.
$\mathrm{Hom}_R(M, N) = \{R\text{-linear maps from } M \text{ to } N\}$. Homomorphisms form an additive group with pointwise addition.
$\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$. The *endomorphisms* form a ring with addition given by pointwise addition and multiplication given by function composition.
$\mathrm{Aut}_R(M) = \mathrm{End}_R(M)^* = \{R\text{-linear isomorphism from } M \text{ to } M\}$. The *automorphisms* form a multiplicative group with multiplication given by function composition.
Examples. Every abelian group M is a $\mathbb{Z}$-module. Choose φ as follows.

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathrm{End}(M). \\ x & \longmapsto & \big(y \mapsto \underbrace{y + \ldots + y}_{x \text{ times}}\big) \end{array}$$

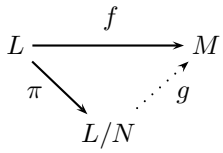
A left ideal of a ring R is an R-module.

Definition 3.6 (Submodule)**.** Let R be a ring and M be an R-module. A *submodule* or *R-submodule* of M is a subgroup N of M such that for all $r \in R, x \in N$ it holds that $rx \in N$.

Let R be a ring and let L and M be R-modules. If N is an R-submodule of M, then the quotient M/N is an R-module by taking $r(x + N) = (rx) + N$ as multiplication. We leave to the reader the verification that the multiplication is well-defined.

Theorem 3.7 (Isomorphism theorem)**.** *Let $f : L \to M$ be an R-linear map. Then $\ker f$ is an R-submodule of L and the image fL is an R-submodule of M. The induced map $L/\ker f \to fL$ is an isomorphism of R-modules.*

Theorem 3.8 (Homomorphism theorem)**.** *Let $f : L \to M$ be an R-linear map and let $N \subset L$ be an R-module with $N \subset \ker f$. Then there exists a unique R-linear map $g : L/N \to M$ such that the following diagram commutes.*



Here π is the canonical map from L to L/N.

Theorem 3.9. *Let K and N be R-submodules of M. Then both $K \cap N$ and $K + N = \{x + y : x \in K, y \in N\}$ are R-submodules of M and the following map is an R-linear isomorphism.*

$$\begin{array}{rcl} K/(K \cap N) & \xrightarrow{\sim} & (K + N)/N \\ x + (K \cap N) & \longmapsto & x + N. \end{array}$$

In order to show how useful modules are, we shall prove the Jordan normal form of matrices over $\mathbb{C}$ by using modules. Firstly, we give two definitions and a theorem.

Let R be a principal ideal domain (PID) and let M be an R-module. For every $x \in M$ we have a homomorphism $g_x : R \to Rx \subset M$ given by $r \mapsto rx$. The kernel of g_x is the *annihilator* of x and it is denoted by $\mathrm{Ann}(x)$. It is an ideal of R. Since R is a principal ideal domain, there exists $y \in R$ such that $\mathrm{Ann}(x) = (y)$.

Definition 3.10 (Order)**.** Let R a principal ideal domain and let M be an R-module. An *order* of an element $x \in M$ is a generator of $\mathrm{Ann}(x)$.

Note that all orders of an element are equal up to multiplication by units of R.

Definition 3.11 (Torsion element)**.** Let R be a principal ideal domain and let M be an R-module. An element $x \in M$ is a *torsion element* if any order of x is not zero, that is $\mathrm{Ann}(x) \neq \{0\}$. Differently stated, an element $x \in M$ is a *torsion element* if there exists $r \in R \setminus \{0\}$ such that $rx = 0$.

If R is a domain ($\neq 0$), then the set of torsion elements of M forms a submodule $T(M) \subseteq M$.

Theorem 3.12 (Structure theorem)**.** *Let R be a principal ideal domain and let M be a finitely generated R-module. Then there exist a natural number r and an R-linear isomorphism*

$$M \cong_R T(M) \oplus R^r.$$

The integer r is called the rank *of M. The module $T(M)$ is isomorphic to $\bigoplus_{\mathfrak{p}} M(\mathfrak{p})$, where $\mathfrak{p}$ runs over all prime ideals of R and all but finitely many $M(\mathfrak{p})$ are 0. Here $M(\mathfrak{p})$ is the submodule of M of elements whose order is a power of $\mathfrak{p}$ and*

$$M(\mathfrak{p}) \cong_R R/\mathfrak{p}^{k_1} \oplus \ldots \oplus R/\mathfrak{p}^{k_m}$$

with $m \geq 0$, $k_1 \geq k_2 \geq \ldots \geq k_m \geq 0 \in \mathbb{Z}$ uniquely determined by $\mathfrak{p}$.

We shall use the structure theorem for finitely generated modules over a principal ideal domain in order to prove the existence of the Jordan normal form.

Let V be a finite-dimensional $\mathbb{C}$-vector space and let $A \in \mathrm{End}(V)$.

The vector space V is a $\mathbb{C}[X]$-module. Firstly, V is a $\mathbb{C}$-vector space and scalar multiplication is a homomorphism $\mathbb{C} \to \mathrm{End}(V)$. Then we extend scalar multiplication to a homomorphism $\varphi : \mathbb{C}[X] \to \mathrm{End}(V)$ by setting $\varphi(X) = A$. The multiplication of an element $x \in V$ by $\sum a_i X^i \in \mathbb{C}[X]$ is given by $(\sum a_i X^i)x = \sum a_i A^i(x)$.

We prove that V is a torsion module. Indeed, if the rank of V was greater than 0, then by Theorem 3.12 the vector space V would have infinite dimension over $\mathbb{C}$, because $\mathbb{C}[X]$ has infinite dimension over $\mathbb{C}$.

Since prime ideals of $\mathbb{C}[X]$ have the form $(X - \lambda)$ for some $\lambda \in \mathbb{C}$, Theorem 3.12 states that V is isomorphic to a direct sum $\bigoplus V_i$, where every V_i is isomorphic to $\mathbb{C}[X]/(X - \lambda_i)^{n_i}$ for some $\lambda_i \in \mathbb{C}$ and $n_i \in \mathbb{Z}_{>0}$. The elements λ_i do not have to be necessarily pairwise distinct.

Choose as a basis of V_i the elements $(X-\lambda_i)^{n_i-1}, (X-\lambda_i)^{n_i-2}, \ldots, (X-\lambda_i), 1$. Multiplication of elements of the basis by $(X - \lambda_i)$ gives $(X - \lambda_i)$ for 1, $(X - \lambda_i)^2$ for $(X - \lambda_i)$, …, $(X - \lambda_i)^{n_i-1}$ for $(X - \lambda_i)^{n_i-2}$ and 0 for $(X - \lambda_i)^{n_i-1}$. Hence, we get the following matrices with respect to the chosen basis for $A - \lambda I$ and A restricted to V_i:

$$A - \lambda I = \begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}, \qquad A = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}.$$

□

Chapter 4

Modules and representation theory

We shall prove that a representation of G on k is a $k[G]$-module.

Definition 4.1 (Group ring)**.** Let R be a ring and G be a group. The *group ring* $R[G]$ of G over R is

$$R[G] = \Big\{ \sum_{\sigma \in G} a_\sigma \sigma : a_\sigma \in R, a_\sigma = 0 \text{ for all but finitely many } \sigma \in G \Big\}.$$

Two elements $\sum_\sigma a_\sigma \sigma$ and $\sum_\sigma b_\sigma \sigma$ are equal if for all $\sigma \in G : a_\sigma = b_\sigma$.

The group ring $R[G]$ is a ring with the following addition and multiplication:

$$\Big(\sum_\sigma a_\sigma \sigma\Big) + \Big(\sum_\sigma b_\sigma \sigma\Big) = \Big(\sum_\sigma (a_\sigma + b_\sigma)\sigma\Big),$$

$$\Big(\sum_\sigma a_\sigma \sigma\Big)\Big(\sum_\sigma b_\sigma \sigma\Big) = \Big(\sum_{\rho \in G} \sum_{\sigma,\tau \in G, \sigma\tau = \rho} (a_\sigma b_\tau)\rho\Big) = \Big(\sum_{\rho \in G} \sum_{\sigma \in G} (a_\sigma b_{\sigma^{-1}\rho})\rho\Big).$$

Note that R is contained in $R[G]$ as a subring ($x \in k \mapsto x \cdot 1 \in R[G]$) and G in $R[G]^*$ as a subgroup ($g \in G \mapsto 1 \cdot g \in R[G]$) if $k \neq \{0\}$.

If we multiply two elements $(\ldots + a\sigma + \ldots)$ and $(\ldots + b\tau + \ldots)$ of $R[G]$, then $(a\sigma)(b\tau) = (ab)(\sigma\tau)$, and therefore $\sigma b = b\sigma$.

The following lemma draws the connection between $k[G]$-modules and representations of G on k.

Lemma 4.2. *Let R be a ring, G be a group, and $R[G]$ be the group ring of G over R. Then an $R[G]$-module is the same as an R-module V with a group homomorphism $G \to \mathrm{Aut}_k(V)$.*

Example. Let k be a field and V be the k-module k^n. Then $\mathrm{End}_k(V) = \mathrm{M}(n,k)$ and $\mathrm{Aut}_k(V) = \mathrm{GL}(n,k)$. A $k[G]$-module structure on V is now given by a homomorphism $G \to \mathrm{GL}(n,k)$.

Proof of Lemma 4.2. We take a k-module V and a group homomorphism $\rho : G \to \mathrm{Aut}_k(V)$. Now we give to V a $k[G]$-module structure by

$$\begin{array}{rcl} k[G] \times V & \longrightarrow & V \\ \Big(\sum\limits_{\sigma \in G}^{<\infty} a_\sigma \sigma\Big) v & \longmapsto & \sum\limits_{\sigma \in G}^{<\infty} a_\sigma \rho(\sigma)(v). \end{array}$$

You can see that it satisfies the axioms of a module.

Conversely, consider a $k[G]$-module W. We make a k-module V by restricting the multiplication to elements in k. Finally, define $\rho : G \to \mathrm{Aut}_k(V)$ by $\rho(\sigma) = (v \in V \mapsto \sigma v)$. □

Now we want to look at the structure of $k[G]$ for two small groups G.

If $G = \{1\}$, then $k[G] = k$.

Let $G = \langle\sigma\rangle$ with $\sigma^2 = 1$ be a group of order 2 and let k be a ring. Consider the following ring homomorphism f:

$$\begin{array}{rcl} f : k[G] & \longrightarrow & k \times k \\ a + b\sigma & \mapsto & (a + b, a - b). \end{array}$$

The kernel of f is $\{a + b\sigma \in k[G] : a = b = -b\}$. If $a + b\sigma$ is an element in the kernel, then $2b = 0$. Now suppose that $2 = 1 + 1 \in k^*$. It follows that $b = 2^{-1}2b = 0$, the kernel of f is $\{0\}$, and hence f is injective.

The ring homomorphism f is surjective if and only if $(1, 0)$ is an element in the image of f. Indeed, $(1, 1)$ is $f(1)$ and $(1, 1)$ and $(1, 0)$ generate together $k \times k$. By definition $(1, 0)$ is an element in the image of f if and only if there exist $a, b \in k$ such that $a + b = 1$ and $a - b = 0$. Thus there exists $a \in k$ such that $2a = 1$. This proves that f is surjective if and only if $2 \in k^*$.

It follows that f is a ring isomorphism if and only if $2 \in k^*$.

Example. Consider $\mathbb{Z}[G]$. Let $f(1) = (1, 1)$ and $f(\sigma) = (1, -1)$. This implies that $(c, d) \in \mathbb{Z}\times\mathbb{Z}$ is in the image of f if and only if $c \equiv d (\mathrm{mod}\, 2)$.

Let R_1 and R_2 be rings, and let $R = R_1 \times R_2$. Let M_1 be an R_1-module, and M_2 an R_2-module. Then $M = M_1 \times M_2$ is an R-module via $(r_1, r_2)(m_1, m_2) = (r_1m_1, r_2m_2)$.

Conversely, every R-module N can be obtained in this (unique) way. Define $M_1 = (1, 0)N = \{(1, 0)x : x \in N\}$. This is an R-submodule of N and it is annihilated by $\{0\} \times R_2$ because $(0, b)(1, 0)x = (0, 0)x = 0$. The kernel of the map $\varphi : R \to \mathrm{End}(M_1)$ obtained by resticting the image of the map $R \to \mathrm{End}(N)$ to $\mathrm{End}(M_1)$ contains $\{0\} \times R_2$. The map φ induces a map from $R/(\{0\} \times R_2) \cong R_1$ to $\mathrm{End}(M_1)$. This makes M_1 into an R_1-module. Analogously, we can define the R_2-module $M_2 = (0, 1)N$. We leave to the reader the verification that the map $M_1 \times M_2 \to N$ given by $(u, v) \mapsto u + v$ is an R-linear isomorphism.

If L_1 is an R_1-module, L_2 is an R_2-module, and $L = L_1 \times L_2$, then there is a map

$$\begin{array}{rcl} \mathrm{Hom}_{R_1}(M_1, L_1) \times \mathrm{Hom}_{R_2}(M_2, L_2) & \longrightarrow & \mathrm{Hom}_R(M, L) \\ (f_1, f_2) & \longmapsto & \big(f : (x, y) \mapsto (f_1(x), f_2(y))\big). \end{array}$$

You can check that it is bijective.

It is straightforward to generalize this result to finite products $R = \prod_{i=1}^n R_i$ of rings.

Now let k be a field of characteristic different from 2 and $G = \langle\sigma\rangle$ be a group of order 2. Then we have a ring isomorphism $k[G] \cong k \times k$ given by $\sigma \mapsto (1, -1)$.

Now suppose that V is a $k[G]$-module, that is a k-vector space V with a k-linear action of G on V. Since every $k[G]$-module V is the product of a k-module V_1 on which σ acts as the identity map and a k-module V_2 on which σ acts as -1, we have the $k[G]$-linear isomorphism $V \cong_{k[G]} V_1 \times V_2$, where $\sigma(v_1, v_2) = (v_1, -v_2)$.

When we have a finite-dimensional representation $\rho : G \to GL(n, k)$ of G over k, we can

therefore choose a basis of V in such a way that we get

$$\rho(\sigma) = \left(\begin{array}{cc|cc} 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \\ \hline & & -1 & 0 \\ & 0 & & \ddots \\ & & 0 & -1 \end{array}\right).$$

More generally, if $G = \langle\sigma\rangle$ is a finite cyclic group with $\sigma^m = 1$, where $m \neq 0$ in k and $X^m - 1$ has m zeros $1, \zeta, \zeta^2, \ldots, \zeta^{m-1}$ in k, then we have the following isomorphism:

$$\begin{array}{rcl} k[G] & \xrightarrow{\sim} & k \times k \times k \times \ldots \times k \\ \sigma & \longmapsto & (1, \zeta, \zeta^2, \ldots, \zeta^{m-1}). \end{array}$$

After a change of basis we can write $\rho(\sigma)$ as

$$\rho(\sigma) = \left(\begin{array}{cc|ccc|ccc} 1 & & 0 & & & & & \\ & \ddots & & & & & 0 & \\ 0 & & 1 & & & & & \\ \hline & & \zeta & & 0 & & & \\ & & & \ddots & & & & \\ & & 0 & & \zeta & & & \\ \hline & & & & & \ddots & & \\ \hline & & & & & & \zeta^{m-1} & & 0 \\ & 0 & & & & & & \ddots & \\ & & & & & & 0 & & \zeta^{m-1} \end{array}\right).$$

Chapter 5

Exact sequences

Definition 5.1. Let R be a ring and let K, L and M be R-modules. A sequence

$$K \xrightarrow{f} L \xrightarrow{g} M$$

is *exact* (at L) if $\ker g = \operatorname{im} f$.

Note that $gf = 0$.

A sequence $K \to L \to M \to N$ is exact if the sequence is exact at L and at M. In general a sequence is exact if it is exact at every point where it is defined.

Examples. $0 \xrightarrow{f} L \xrightarrow{g} M$ is exact if and only if $\ker g = 0$ if and only if g is injective.

$K \xrightarrow{f} L \xrightarrow{g} 0$ is exact if and only if $\operatorname{im} f = L$ if and only if f is surjective.

$K \xrightarrow{f} 0 \xrightarrow{g} M$ is always exact.

$0 \xrightarrow{f} L \xrightarrow{g} 0$ is exact if and only if $L = 0$.

$0 \longrightarrow L \xrightarrow{f} M \longrightarrow 0$ is exact if and only if f is an isomorphism.

$0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \longrightarrow 0$ is exact if and only if K can be seen (via f) as a submodule of L and M can be identified (via g) with L/K.

$0 \longrightarrow K \xrightarrow{f} L \xrightarrow{g} M \xrightarrow{h} N \longrightarrow 0$ is exact if and only if K is isomorphic to $\ker g$ and N is isomorphic to $\operatorname{coker} g$. ($\operatorname{coker} g = M/(\operatorname{im} g)$ is the *cokernel* of g.)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & K \oplus M & \xrightarrow{p} & M & \longrightarrow & 0 \\ & & x & \longmapsto & (x,0) & & & & \\ & & & & (x,y) & \longmapsto & y & & \end{array} \qquad \text{is exact.}$$

Definition 5.2. A short exact sequence $0 \to K \to L \to M \to 0$ *splits* if there exists a homomorphism $h : L \to K \oplus M$ such that the following diagram commutes.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & L & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_K} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle id_M} & & \\ 0 & \longrightarrow & K & \xrightarrow{i} & K \oplus M & \xrightarrow{p} & M & \longrightarrow & 0. \end{array}$$

Lemma 5.3 (Snake Lemma)**.** *Consider the following commutative diagram where the rows are exact:*

$$\begin{array}{ccccccccc} & & K_1 & \longrightarrow & L_1 & \longrightarrow & M_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & K_2 & \longrightarrow & L_2 & \longrightarrow & M_2. & & \end{array}$$

Then there is an exact sequence $\ker f \to \ker g \to \ker h \to \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h$.

Furthermore, if the morphism $K_1 \to L_1$ *is injective, then so is the morphism* $\ker f \to \ker g$, *and if the morphism* $L_2 \to M_2$ *is sujective, then so is the morphism* $\operatorname{coker} g \to \operatorname{coker} h$.

Let I be an index set, R be a ring and M_i an R-module for every $i \in I$.

The *direct sum* is

$$\bigoplus_{i\in I} M_i = \{(x_i)_{i\in I} : x_i \in M_i \text{ for all } i \in I, \{i \in I : x_i \neq 0\} \text{ is finite}\}$$

and the *direct product* is

$$\prod_{i\in I} M_i = \{(x_i)_{i\in I} : x_i \in M_i \text{ for all } i \in I\}.$$

The direct sum is an R-submodule of the direct product. Note that $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$ if and only if $M_i = 0$ for all but finitely many $i \in I$.

A direct sum $\bigoplus_{i\in I} M$ is also written as $M^{(I)}$ and the direct product $\prod_{i\in I} M$ as M^I.

We shall introduce some properties of modules.

Definition 5.4. An R-module F is *free* is there is a set I such that $R^{(I)} \cong F$.

For every $j \in I$ we call e_j the image of $(\ldots, 0, 1, 0, \ldots) \in R^{(I)}$ under this isomorphism, where the 1 is at the j position. The elements e_j form a *basis* of F over R. This means that for every $x \in F$ there is a unique sequence of elements $(r_j)_{j\in I}$ with $r_j \in R$ and $r_j = 0$ for all but finitely many $j \in I$ such that $x = \sum_{i\in I} r_j e_j$.

Hence F is a free R-module if and only if F has an R-basis.

If R is a *division ring*, then every R-module is free. (A division ring is a ring where $1 \neq 0$ and every nonzero element has a left multiplicative inverse).

Lemma 5.5. *Let* $0 \to K \to L \to F \to 0$ *be a short exact sequence and let* F *be a free module. Then the sequence splits.*

Definition 5.6. Projective module Let R be a ring. An R-module M is a *projective R-module* if every short exact sequence $0 \to K \to L \to M \to 0$ of R-modules splits.

Definition 5.7. Injective module Let R be a ring. An R-module M is an *injective R-module* if every short exact sequence $0 \to M \to N \to P \to 0$ of R-modules splits.

Definition 5.8. Semisimple module Let R be a ring. An R-module M is a *semisimple R-module* if every short exact sequence $0 \to L \to M \to N \to 0$ of R-modules splits.

Example. Let $R = \mathbb{Z}$. An R-module M is projective if and only if M is free. An R-module M is injective if and only if M is divisible. An R-module M is semisimple if and only if the order of every $x \in M$ is finite and square-free.

Definition 5.9. Finitely generated module An R-module M is a *finitely generated R-module* if there exist $n \in \mathbb{Z}_{\geq 0}$ and a surjective R-linear map $R^n \to M$.

An equivalent definition is that an R-module M is finitely generated if there are elements $a_1, \ldots, a_n$ such that for all $x \in M$ there exist $r_1, \ldots r_n \in R : x = r_1 a_1 + \ldots + r_n a_n$. The elements $r_1, \ldots, r_n$ are not necessarily unique. If they are unique for all x in M, then M is free.

Chapter 6

Homomorphisms and tensors

Let R be a ring and M and N two R-modules.

The R-linear maps from M to N form an abelian group $\mathrm{Hom}_R(M,N)$ via $(f_1+f_2)(x) = f_1(x)+f_2(x) \in N$.

In general $\mathrm{Hom}_R(M,N)$ is not an R-module. Indeed, if f is an R-linear map from M to N, then rf is not necessarily R-linear. We have $(rf)(sx) = r(f(sx)) = rsf(x)$, but this is not always equal to $s(rf(x)) = srf(x)$. However, if R is commutative, then $\mathrm{Hom}_R(M,N)$ is an R-module.

Let R, S and T be rings, M be an R-S-bimodule and N be an R-T-bimodule. Then ${}_R\mathrm{Hom}(M,N)$ is an S-T-bimodule via $(sf)(x) = f(xs)$ and $(ft)(x) = f(x)t$. We write R as subscript on the left, because we want to remark that M and N are left R-modules.

Let L be a U-S-bimodule. Similarly, $\mathrm{Hom}_S(M,L)$ is a U-R-bimodule.

Let $f : N \to N'$ be an R-T-linear map. It induces an S-T-linear map f_* given by:

$$\begin{array}{rcl} {}_R\mathrm{Hom}(M,N) & \xrightarrow{f_*} & {}_R\mathrm{Hom}(M,N') \\ (M \xrightarrow{g} N) & \longmapsto & (M \xrightarrow{fg} N'). \end{array}$$

Note that fg is the composition of R-linear maps, thus it is also R-linear. The map f_* is called *the map induced by* f or ${}_R\mathrm{Hom}(M,f)$.

Now let $h : M \to M'$ be an R-S-linear map. It induces an S-T-linear map h^* given by:

$$\begin{array}{rcl} {}_R\mathrm{Hom}(M,N) & \xleftarrow{h^*} & {}_R\mathrm{Hom}(M',N) \\ (M \xrightarrow{gh} N) & \longmapsto & (M' \xrightarrow{g} N). \end{array} \tag{6.1}$$

We also write the map h^* as ${}_R\mathrm{Hom}(h,N)$.

Using the terminology of category theory we say that ${}_R\mathrm{Hom}(M,-)$ is *covariant* and ${}_R\mathrm{Hom}(-,N)$ is *contravariant*. The arguments can be modules or maps.

Let f and f' be R-T-linear maps such that

$$N \xrightarrow{f} N' \xrightarrow{f'} N''.$$

Then

$${}_R\,\mathrm{hom}(M,N) \xrightarrow{f_*} {}_R\mathrm{Hom}(M,N') \xrightarrow{f'_*} {}_R\mathrm{Hom}(M,N'')$$

and $f'_*f_* = (f'f)_*$.

Let h and h' be R-S-linear maps such that

$$M \xrightarrow{h} M' \xrightarrow{h'} M''.$$

Then

$$ {}_R\mathrm{Hom}(M,N) \xleftarrow{h^*} {}_R\mathrm{Hom}(M',N) \xleftarrow{h'^*} {}_R\mathrm{Hom}(M'',N)$$

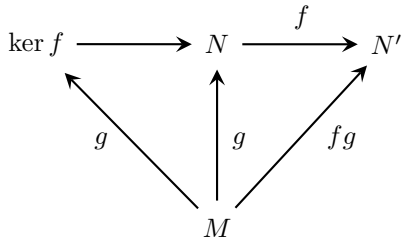
and $h^*h'^* = (h'h)^*$.

Thus, ${}_R\mathrm{Hom}(M,N)$ is 'contra' in M an 'co' in N and therefore it is an S-T-bimodule. Similarly, ${}_S\mathrm{Hom}(M,L)$ is 'contra' in M and 'co' in L and therefore it is a U-R-bimodule.

Let R be a ring and let M be an R-module. We will show that "${}_R\mathrm{Hom}(M,-)$ transforms kernels into kernels". More precisely, we have the following lemma.

Lemma 6.1. *Let N and N' be R-modules and let the map $f : N \to N'$ be R-linear. Then ${}_R\mathrm{Hom}(M, \ker f) = \ker({}_R\mathrm{Hom}(M,f)) = \ker f^*$.*

Proof. Every R-linear homomorphism g from M to $\ker f$ is also an R-linear homomorphism from M to N, because $\ker f \subset N$. We have the following commutative diagram.



We see that $g(M) \subset \ker f \Leftrightarrow fg = 0 \Leftrightarrow g \in \ker f_*$. Hence ${}_R\mathrm{Hom}(M, \ker f) = \ker f_*$. □

We say that ${}_R\mathrm{Hom}(M,-)$ is *left exact*, because if the sequence $0 \longrightarrow N''' \xrightarrow{f''} N \xrightarrow{f} N'$ is exact then the sequence $0 \longrightarrow {}_R\mathrm{Hom}(M,N''') \xrightarrow{f''_*} {}_R\mathrm{Hom}(M,N) \xrightarrow{f_*} {}_R\mathrm{Hom}(M,N'')$ is also exact.

Furthermore, we have

$$ {}_R\mathrm{Hom}(M, N''' \oplus N') \cong {}_R\mathrm{Hom}(M,N''') \oplus {}_R\mathrm{Hom}(M,N').$$

The analogous statement is true for ${}_R\mathrm{Hom}(-,N)$.

Since R itself is an R-R-bimodule, both R and N are left R-module. The map

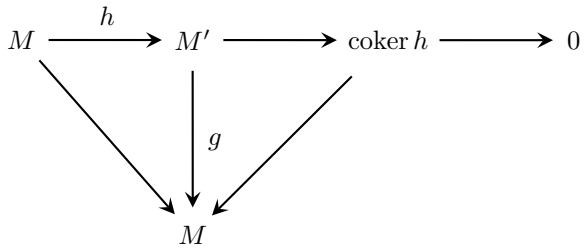
$$\begin{array}{rcl} {}_R\mathrm{Hom}(R,N) & {}_R\cong & N \\ f & \longmapsto & f(1) \end{array}$$

is an R-isomorphism, because the map $N \to {}_R\mathrm{Hom}(R,N)$ given by $x \mapsto (r \mapsto rx)$ is the inverse map.

Let R be a ring and let N be an R-module. We will show that "${}_R\mathrm{Hom}(-,N)$ transforms cokernels into cokernels". More precisely, the following lemma holds.

Lemma 6.2. *Let M and M' be R-modules and let the map $h : M \to M'$ be R-linear. Then ${}_R\mathrm{Hom}(\mathrm{coker}\, h, N) = \ker({}_R\mathrm{Hom}(h,N)) = \ker h^*$.*

Proof. Since $\mathrm{coker}\, h$ is isomorphic to $M'/h(M)$, the projection map is a surjective map from M' to $\mathrm{coker}\, h$. Now let $g : M' \to N$ be an R-linear homomorphism. We have the following diagram.



If g factors through $\operatorname{coker} h$, that is the diagram above commutes, then there is an R-linear homomorphism $\operatorname{coker} h \to N$ associated with g. This is equivalent to the fact that $gh = 0$, that is $h^*(g) = 0$. □

We say that ${}_R\mathrm{Hom}(-, N)$ is *left exact*, because if the sequence $M \xrightarrow{h} M' \xrightarrow{h'} M'' \to 0$ is exact then the sequence $0 \to {}_R\mathrm{Hom}(M'', N) \xrightarrow{h'^*} {}_R\mathrm{Hom}(M', N) \xrightarrow{h^*} {}_R\mathrm{Hom}(M, N)$ is also exact.

If we consider two free R-module R^n and R^m, then we see that ${}_R\mathrm{Hom}(R^n, R^m)$ is isomorphic to the set of $m \times n$-matrices over R.

Let S and T be sets. The set of functions from T to S may be denoted by $\mathrm{Map}(T, S)$ or S^T or $\prod_{t \in T} S$. This notation suggests that $(S^T)^U = S^{T \times U}$, where U is also a set. Indeed, it is true, because the function

$$\begin{array}{rcl} \mathrm{Map}(T \times U, S) & \longrightarrow & \mathrm{Map}(U, \mathrm{Map}(T, S)) \\ f & \longmapsto & (u \mapsto (t \mapsto f(t, u))) \end{array}$$

is bijective.

Let L, M and N be abelian group. First we give a definition.

Definition 6.3. A function $f : L \times M \to N$ is *bilinear* if for all $x, x_1, x_2 \in L$ and for all $y, y_1, y_2 \in M$ it holds that $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$ and $f(x_1 + x_2, y) = f(x, y_1) + f(x, y_2)$.

We have

$$\mathrm{Hom}(L, \mathrm{Hom}(M, N)) \subset \mathrm{Map}(L, \mathrm{Hom}(M, N)) \subset \mathrm{Map}(L, \mathrm{Map}(M, N)) = \mathrm{Map}(L \times M, N).$$

If $f : L \times M \to N$ is a function, then the corresponding element of $\mathrm{Map}(L, \mathrm{Map}(M, N))$ belongs to $\mathrm{Hom}(L, \mathrm{Hom}(M, N))$ if and only if f is bilinear.

We denote the set of bilinear functions from $L \times M$ to N by $\mathrm{Bil}(L \times M, N)$. The set $\mathrm{Bil}(L \times M, N)$ is a group. We have

$$\mathrm{Hom}(L, \mathrm{Hom}(M, N)) = \mathrm{Bil}(L \times M, N) = \mathrm{Hom}(L \otimes M, N).$$

We will soon see what $L \otimes M$ means.

Let R be a ring, L be a right R-module, M be a left R-module and N be an abelian group. We extend the definition of bilinear functions to R-bilinear maps.

Definition 6.4. A map $f : L \times M \to N$ is R-bilinear if f is a bilinear function and for all $r \in R$, $x \in L$ and $y \in M$ we have $f(xr, y) = f(x, ry)$.

Note that being $\mathbb{Z}$-bilinear is the same as being bilinear.

Example. The map $R \times R \to R$ given by $(s, t) \mapsto st$ is R-bilinear.

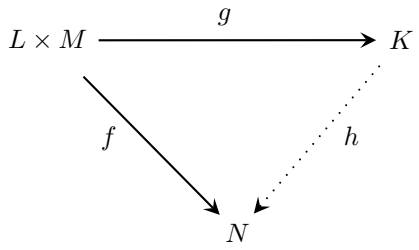
The map $R \times M \to M$ given by $(s, m) \mapsto sm$ is R-bilinear.

The map $L \times R \to L$ given by $(l, t) \mapsto lt$ is R-bilinear.

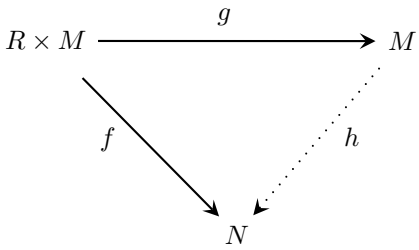
Definition 6.5 (Universal map)**.** Let K be an abelian group. An R-bilinear map $g : L \times M \to K$ is an *universal map* if for every abelian group N the map

$$\begin{array}{ccc} \mathrm{Hom}(K, N) & \longrightarrow & \mathrm{Bil}_R(L \times M, N) \\ h & \longmapsto & hg \end{array}$$

is bijective. In other words, g is a universal map if for every abelian group N and for every R-bilinear map $f : L \times M \to N$ there is a unique group homomorphism $h : K \to N$ which make the following diagram commute.



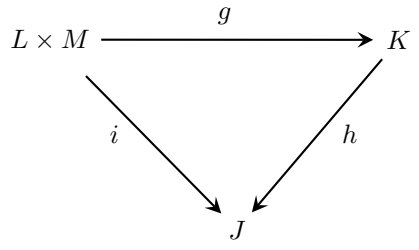
Example. All the three examples we have just seen are universal. We are going to prove it in the case of the map $R \times M \to M$ given by $(s, m) \mapsto sm$. We have to show that there exists a group homomorphism $h : M \to N$ such that the following diagram commutes.



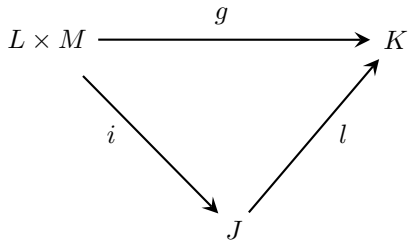
If such a homomorphism h exists, then we have $f(s, m) = hg(s, m) = h(sm) = hg(1, sm) = f(1, sm)$. Hence, it has to be defined by $h(m) = f(1, m)$. The map defined in this way is a group homomorphism. Since $f(s, m) = f(1, sm) = h(sm)$, the map g is universal.

Theorem 6.6. *Let $g : L \times M \to K$ and $i : L \times M \to J$ be R-bilinear and universal maps.Then there is a unique group isomorphism $h : K \xrightarrow{\sim} J$ such that $h \circ g = i$.*

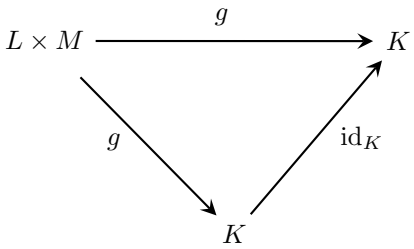
Proof. Because of the universality of g there exists a group homomorphism $h : K \to J$ which make the following diagram commute.



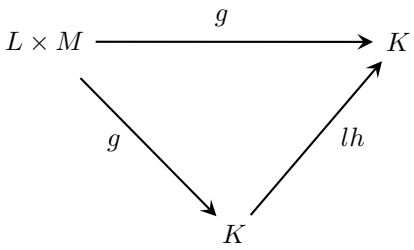
We have to show that h is bijective. Since i is also universal, there is also a group homomorphism $l : J \to K$ which make the following diagram commute.



Now we know that $i = h \circ g$ and $g = l \circ i$. We will prove that $h \circ l = \mathrm{id}_J$ and $l \circ h = \mathrm{id}_K$. Look at the following commutative diagram.



Since $l \circ h \circ g = l \circ i = g$, the following diagram commutes too.



The universality of g implies that $l \circ h = \mathrm{id}_K$. Similarly, we can prove that $h \circ l = \mathrm{id}_J$. Hence l is the inverse of h and thus h is an isomorphism between K and J such that $h \circ g = i$. □

Definition 6.7. If there exists a universal R-bilinear map $g : L \times M \to K$, then we define

$$\begin{array}{rcl} L \otimes_R M & := & K \\ \cup & & \cup \\ x \otimes y & := & g(x, y). \end{array}$$

Note that $(L \otimes_R M, - \otimes -)$ is defined up to isomorphism.

If we have a pair (K, g), then it is uniquely determined up to isomorphism and we write $L \otimes_R M$ and $x \otimes y$ instead of K and $g(x, y)$.

Example. $R \otimes_R R \cong R$ via $x \otimes y \leftrightarrow xy$.

$R \otimes_R M \cong M$ via $r \otimes y \leftrightarrow ry$.

$L \otimes_R R \cong L$ via $x \otimes r \leftrightarrow xr$.

It is true that "$\otimes$ commutes with arbitrary direct sums". More precisely, we have the following lemma.

Lemma 6.8. *Let $(M_i)_{i\in I}$ be family of R-modules and suppose that for every $i \in I$ the tensor product $L \otimes_R M_i$ exists. Then $L \otimes_R (\bigoplus_{i\in I} M_i)$ also exists and*

$$\begin{array}{ccc} L \otimes_R (\bigoplus_{i\in I} M_i) & \xrightarrow{\sim} & \bigoplus_{i\in I}(L \otimes_R M_i) \\ x \otimes (y_i)_{i\in I} & \longmapsto & (x \otimes y_i)_{i\in I}. \end{array}$$

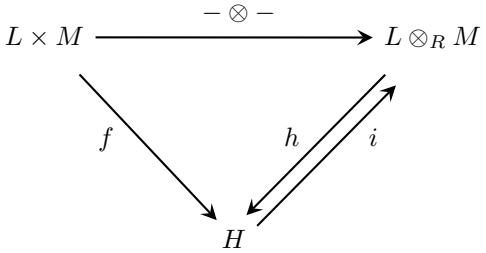
Proof. Check by yourself that the map

$$\begin{array}{ccc} L \times (\bigoplus_{i\in I} M_i) & \longrightarrow & \bigoplus_{i\in I}(L \otimes_R M_i) \\ (x, (y_i)_{i\in I}) & \longmapsto & (x \otimes y_i)_{i\in I} \end{array}$$

is R-bilinear and universal. □

Theorem 6.9. *If $L \otimes_R M$ exists, then it is generated by $\{x \otimes y | x \in L, y \in M\}$.*

Proof. Let H the subgroup of $L \otimes_R M$ generated by $\{x \otimes y | x \in L, y \in M\}$. We have the following diagram.



.

By definition of map we have $i \circ f = - \otimes -$. The universality of $\otimes_R$ implies that $f = h \circ (- \otimes -)$. Therefore the diagram commutes. Now we see that $i \circ h \circ (- \otimes -) = - \otimes - = \mathrm{id}(- \otimes -)$. The unicity of h gives $i \circ h = \mathrm{id}_{L\otimes_R M}$. Thus the inclusion i is surjective and $H = L \otimes_R M$. □

Example. Let L be a right R-module. Then

$$\begin{array}{ccccc} L \otimes_R (R^n) & \cong (L \otimes_R R)^n \cong & L^n \\ x \otimes (r_i)_{i=1}^n & \longmapsto & (xr_i)_{i=1}^n. \end{array}$$

In particular:

$$\begin{array}{ccc} (R^m) \otimes (R^n) & \cong & R^{mn} \\ (b_j)_{j=1}^m \otimes (a_i)_{i=1}^n & \longmapsto & (b_j a_i)_{1\le i\le n, 1\le j\le m}. \end{array}$$

Example. Let k be a field and let V and W be two finite-dimensional k-vector spaces. We write $V \cong k^m$ and $W \cong k^n$, with bases $\{e_1, \ldots, e_m\}$ and $\{f_1, \ldots, f_n\}$, respectively. Then $V \otimes_k W$ is a k-vector space of dimension mn with basis $(e_i \otimes f_j)_{1\le i\le m, 1\le j\le n}$.

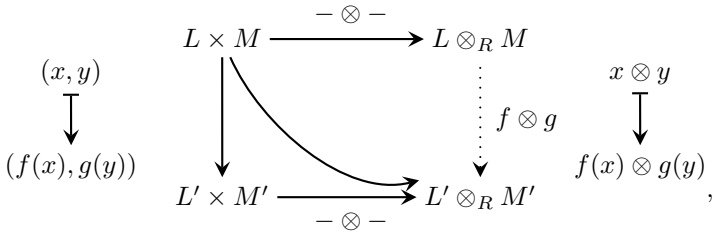
Let R, S, and T be rings. Let L be an S-R-bimodule and M be an R-T-bimodule. Then $L \otimes_R M$ is an S-T-bimodule via $s(x \otimes y) = (sx) \otimes y$ and $(x \otimes y)t = x \otimes (yt)$.

Let R be a ring, L be a right R-module and M be a left R-module. If R is commutative, then $L \otimes_R M$ is an R-module with $r(x \otimes y) = (rx) \otimes y = (xr) \otimes y = x \otimes (ry)$ and $(x \otimes y)r = x \otimes (yr)$. Moreover, $L \otimes_R M \cong M \otimes_R L$.

Let R, S, T, and U be rings and let L be an S-R-bimodule, M be an R-T-bimodule, and N be a T-U-bimodule. Then

$$(L \otimes_R M) \otimes_T N_S \cong_U L \otimes_R (M \otimes_T N).$$

Suppose that $f : L \to L'$ is a right R-linear map and $g : M \to M'$ is an R-linear map. Then the following diagram commutes.



where the map $L \times M \to L' \otimes_R M'$ is bilinear via $L' \times M'$.

For instance, if we take $L' = L$ and $f : L \to L$ to be the identity map id_L, we have the following map:

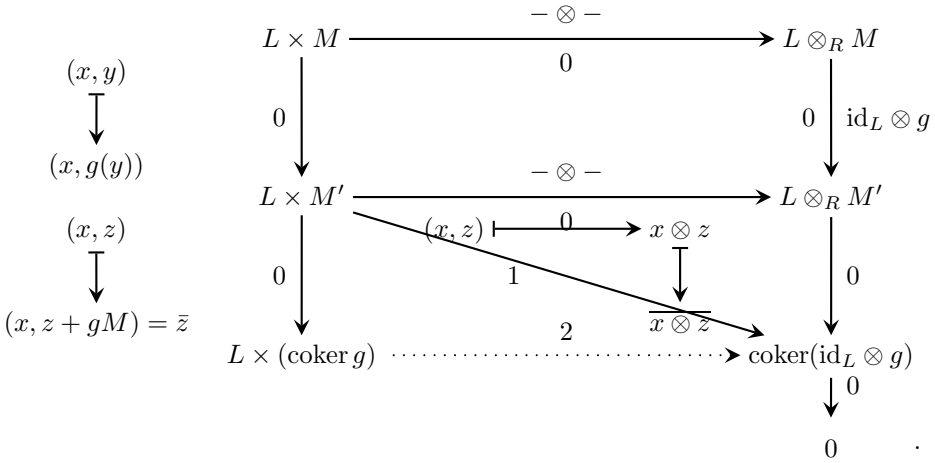
$$\begin{array}{ccc} L \otimes_R M & \xrightarrow{\mathrm{id}_L \otimes g} & L \otimes_R M' \\ x \otimes y & \longmapsto & x \otimes g(y). \end{array}$$

We say that "$L \otimes_R -$ commutes with cokernels". More precisely, we have the following theorem.

Theorem 6.10. *Let $g : M \to M'$ be R-linear and suppose that both $L \otimes_R M$ and $L \otimes_R M'$ exist. Then $L \otimes_R (\operatorname{coker} g)$ and $L \otimes_R (\operatorname{coker} g) = \operatorname{coker}(\mathrm{id}_L \otimes g)$ also exist.*

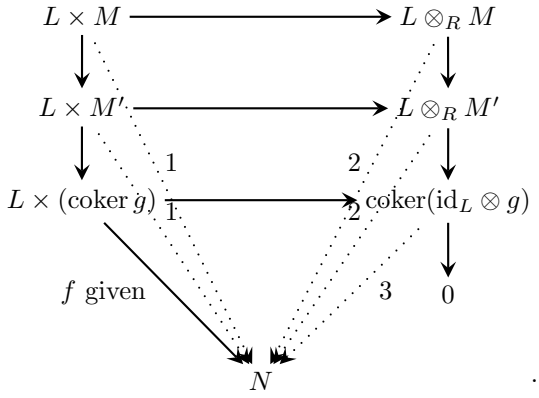
In other words, $L \otimes_R -$ is right exact.

Proof. Diagram chasing! We already have all the maps where there is 0. The map with 1 can be constructed by composition. The map with 2 can be obtained by sending $(x, \bar{z})$ to $\overline{x \otimes z}$. This map is well-defined, because if $(x, \bar{z})$ and $(x\overline{z'})$ represent the same class then $\overline{x \otimes z}$ and $\overline{x \otimes z'}$ are equal. Indeed, $z' - z \in \operatorname{im} g$, thus $\overline{x \otimes (z' - z)} = 0$, because the right column is exact.



Let N be an abelian group and suppose we are given $f : L \times (\operatorname{coker} g) \to N$. Then there are bilinear maps $L \times M \to N$ and $L \times M' \to N$ which are obtained by composition (they are labeled with 1 in the next diagram). The map $L \times M \to N$ we get in this way is therefore the zero map, because the left column is exact in the second component.

From the universality of these two maps it follows that there are unique maps $L \otimes_R M \to N$ and $L \otimes_R M' \to N$ (these are labeled with 2). There is also a map $\operatorname{coker}(\mathrm{id}_L \otimes g) \to N$, because the map $L \otimes_R M' \to \operatorname{coker}(\mathrm{id}_L \otimes g)$ is surjective and for every element of $\operatorname{coker}(\mathrm{id}_L \otimes g)$ we can take a preimage in $L \otimes_R M'$ and then looking at its image in N. This map is independent of the choice of the preimage, because the rightcolumn is exact and therefore the map $L \otimes_R M \to N$ is the zero map. We label this new map with 3. Since the map $L \otimes_R M' \to N$ is unique, then the map 3 is also unique.



Furthermore, we have that $L \otimes_R -$ is right exact, because if the sequence $M \xrightarrow{g} M' \to M'' \to 0$ is exact then the sequence $L \otimes_R M \to L \otimes_R M' \to L \otimes_R M'' \to 0$ is also exact. □

We have not yet proven that $L \otimes_R M$ exists.

Theorem 6.11. *The tensor product $L \otimes_R M$ exists.*

Proof. Choose a subset $S \subset M$ which generates M, that is a subset S such that the R-linear map

$$\begin{aligned} R^{(S)} = \bigoplus_{s \in S} R &\longrightarrow M \\ (r_s)_{s \in S} &\longmapsto \sum_{s \in S} r_s s \end{aligned}$$

is surjective. Choose a subset $T \subset \ker g$ which generates $\ker g$, that is the analogous map $R^{(T)} \to \ker g$ is surjective. Now the sequence $R^{(T)} \xrightarrow{h} R^{(S)} \to M = \operatorname{coker} h \to 0$ is exact. Both $L \otimes_R R^{(T)}$ and $L \otimes_R R^{(S)}$ exist, then the previous theorem says that $L \otimes_R M$ also exists. □

Example. We show that $V_4 \otimes_{\mathbb{Z}} C_8 = V_4$. The sequence $\mathbb{Z} \xrightarrow{8} \mathbb{Z} \to C_8 \to 0$ is exact, thus

$$\begin{aligned} V_4 \otimes \mathbb{Z} &\xrightarrow{\mathrm{id}_{V_4} \otimes 8} V_4 \otimes \mathbb{Z} \longrightarrow V_4 \otimes C_8 \longrightarrow 0 \\ x \otimes y &\longmapsto 8(x \otimes y) \end{aligned}$$

is exact. We know that $V_4 \otimes \mathbb{Z} = V_4$ and that $x \otimes y \mapsto 8(x \otimes y)$ is the zero map. Now it follows that $V_4 \otimes C_8 = V_4$.

If we take the tensor product between V_4 and another abelian group, we sometimes get the trivial group: $V_4 \otimes C_9 = 0$.

Definition 6.12 (Divisible group)**.** An abelian group G is a *divisible group* if for every $x \in G$ and every $n \in \mathbb{Z}$ there exists $y \in G$ such that $ny = x$.

Definition 6.13 (Torsion group)**.** An abelian group G is a *torsion group* if for every $z \in G$ there exists $m \in \mathbb{Z}_{>0}$ such that $mz = 0$.

Theorem 6.14. *Let A be a divisible group and let B be a torsion group. Then $A \otimes_{\mathbb{Z}} B = 0$.*

Proof. Let $x \in A$ and $z \in B$ be arbitrary elements. Choose $m \in \mathbb{Z}_{>0}$ in such a way that $mz = 0$. Since A is divisible, there is $y \in A$ such that $x = my$. Hence $x \otimes z = (my) \otimes z = y \otimes (mz) = y \otimes 0 = 0$. □

Example. $\mathbb{Q} \otimes C_{36} = 0$
$(\mathbb{Q}/\mathbb{Z}) \otimes (\mathbb{Q}/\mathbb{Z}) = 0$
$(\mathbb{Q}/\mathbb{Z}) \otimes (\mathbb{R}/\mathbb{Z}) = 0$
Let L, M, and N be abelian groups. Since both $\mathrm{Hom}(L, \mathrm{Hom}(M, N))$ and $\mathrm{Hom}(L \otimes M, N)$ are isomorphic to $\mathrm{Bil}(L \times M, N)$, we have

$$\mathrm{Hom}(L, \mathrm{Hom}(M, N)) \cong \mathrm{Hom}(L \otimes M, N).$$

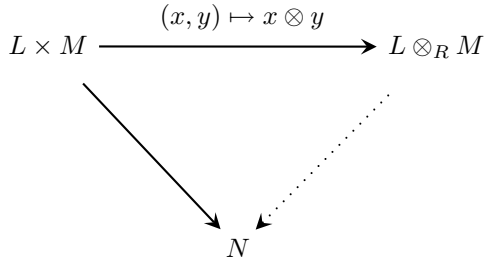
Moreover,

$$\underbrace{{}_S\mathrm{Hom}(\underbrace{L}_{S-U}, \underbrace{{}_R\mathrm{Hom}(\underbrace{M}_{R-S}, \underbrace{N}_{R-T})}_{S-T})_U}_{U-T} \cong_T \underbrace{{}_R\mathrm{Hom}(\underbrace{\underbrace{M}_{R-S} \otimes_S \underbrace{L}_{S-U}}_{R-U}, \underbrace{N}_{R-T})}_{U-T} \tag{6.2}$$

and

$$\underbrace{\mathrm{Hom}(\underbrace{L}_{U-S}, \underbrace{\mathrm{Hom}_R(\underbrace{M}_{S-R}, \underbrace{N}_{T-R})}_{T-S})_T}_{T-U} \cong_U \underbrace{\mathrm{Hom}_R(\underbrace{\underbrace{L}_{U-S} \otimes_S \underbrace{M}_{S-R}}_{U-R}, \underbrace{N}_{T-R})}_{T-U}. \tag{6.3}$$

Let R be a ring, L be a right R-module and M be a left R-module. Then we have the following commutative diagram.



If M is an R-T-bimodule and L is an S-R-bimodule, then $L \otimes_R M$ is an S-T-bimodule.

Let k be a field and let V and W be finite-dimensional k-vector spaces of dimension m and n, respectively. Then $\dim_k(V \otimes_k W) = nm$.

Let R and R' be two rings, $R \to R'$ be a ring homomorphism and M be an R-module. Then $M' := \underbrace{R'}_{R'-R} \otimes_R \underbrace{M}_{R-\mathbb{Z}}$ is an R'-module. We say that M' is obtained by *base extension.*

If M is free over R, then M' is also free over R'.

Example. Consider the ring homomorphism $\mathbb{R} \to \mathbb{C}$. Let V be an $\mathbb{R}$-vector space which is isomorphic to $\mathbb{R}^n$ as an $\mathbb{R}$-module. Let $(e_i)_{i=1}^n$ be a basis of V. Then $\mathbb{C} \otimes_{\mathbb{R}} V \cong \mathbb{C}^n$ as a $\mathbb{C}$-module with basis $(1 \otimes e_i)_{i=1}^n$.

Lemma 6.15. *Let $g_1 : R \to R_1$ and $g_2 : R \to R_2$ be ring homomorphisms with $g_1(R) \subset Z(R_1)$ and $g_2(R) \subset Z(R_2)$. Then $R_1 \otimes_R R_2$ is a ring via $(s_1 \otimes s_2) \cdot (t_1 \otimes t_2) = (s_1 t_1) \otimes (s_2 t_2)$.*

Sketch of the proof. It is sufficient to show that there exists a map

$$(R_1 \otimes_R R_2) \times (R_1 \otimes_R R_2) \xrightarrow{\times} R_1 \otimes_R R_2$$

such that

$$(s_1 \otimes s_2, t_1 \otimes t_2) \longmapsto (s_1 t_1) \otimes (s_2 t_2).$$

Step 1. Define

$$\begin{array}{rcl} R_1 \times R_2 \times R_1 \times R_2 & \xrightarrow{f} & R_1 \otimes_R R_2 \\ (s_1, s_2, t_1, t_2) & \longmapsto & (s_1 t_1) \otimes (s_2 t_2). \end{array}$$

Step 2. Check that for every $s_1 \in R_1$ and every $s_2 \in R_2$ the map

$$f(s_1, s_2, -, -) : R_1 \times R_2 \longrightarrow R_1 \otimes_R R_2$$

is R-bilinear. For every $(s_1, s_2) \in R_1 \times R_2$ the universal property gives a unique homomorphism

$$\begin{array}{rcl} h_{s_1,s_2} : R_1 \otimes_R R_2 & \longrightarrow & R_1 \otimes_R R_2 \\ t_1 \otimes t_2 & \longmapsto & (s_1 t_1) \otimes (s_2 t_2). \end{array}$$

Step 3. Check that the map

$$\begin{array}{rcl} R_1 \times R_2 & \longrightarrow & \mathrm{Hom}(R_1 \otimes_R R_2, R_1 \otimes_R R_2) \\ (s_1, s_2) & \longmapsto & h_{s_1,s_2} \end{array}$$

is R-bilinear. Then we get

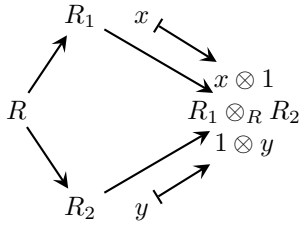
$$\begin{array}{rcl} g : R_1 \otimes_R R_2 & \longrightarrow & \mathrm{Hom}(R_1 \otimes_R R_2, R_1 \otimes_R R_2) \\ s_1 \otimes s_2 & \longmapsto & h_{s_1,s_2}. \end{array}$$

Step 4. Define $\times$ by

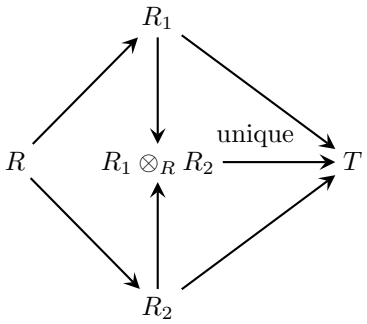
$$\times(a, b) = (g(a))(b).$$

□

We have the following commutative diagram of ring homomorphisms.

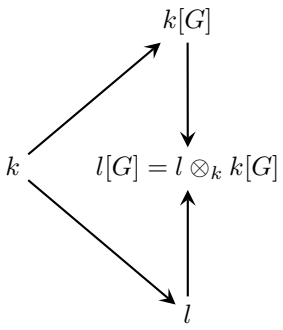


Let R, R_1, and R_2 be commutative rings and let $R \to R_1$ and $R \to R_2$ be ring homomorphisms. Let T be a ring and let $R_1 \to T$ and $R_2 \to T$ be ring homomorphisms. Then the following diagram commutes.



If $R \to R_1 \to T$ and $R \to R_2 \to T$ are the same ring homomorphism $R \to T$, then it goes through the tensor product.

Now we look at a case which is relevant to representation theory. Let k be a field and let l be an extension field of k. We take the group ring $k[G]$ as R_1 and l as R_2. Then the following diagram commutes.



Chapter 7

Jordan-Hölder Theorem and Grothendieck groups

The results of this chapter are relatively recent and they have been found by the following mathematicians: Camille Jordan (1838–1921), Otto Hölder (1859–1937), Otto Schreier (1901–1929), Hans Zassenhaus (1912–1991), and Alexander Grothendieck (1928).

Let R be a ring and M be an R-module. We look at *chains* in M.

Definition 7.1 (Chain)**.** A *chain* for M is sequence of submodules

$$\{0\} = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_t = M,$$

where $t \in \mathbb{Z}_{\geq 0}$. The number t is the *length* of the chain.

Definition 7.2 (Isomorphism)**.** Let $(M_i)_{i=0}^t$ be a chain for M and $(N_j)_{j=0}^u$ be a chain for N. An *isomorphism* from the first chain to the second one is a bijection

$$\rho : \{1, 2, \ldots, t\} \longrightarrow \{1, 2, \ldots, u\}$$

plus for every $i \in \{1, 2, \ldots, t\}$ an R-isomorphism

$$M_i/M_{i-1} \xrightarrow{\sim} N_{\rho(i)}/N_{\rho(i)-1}.$$

It is clear that isomorphic chains have the same length.

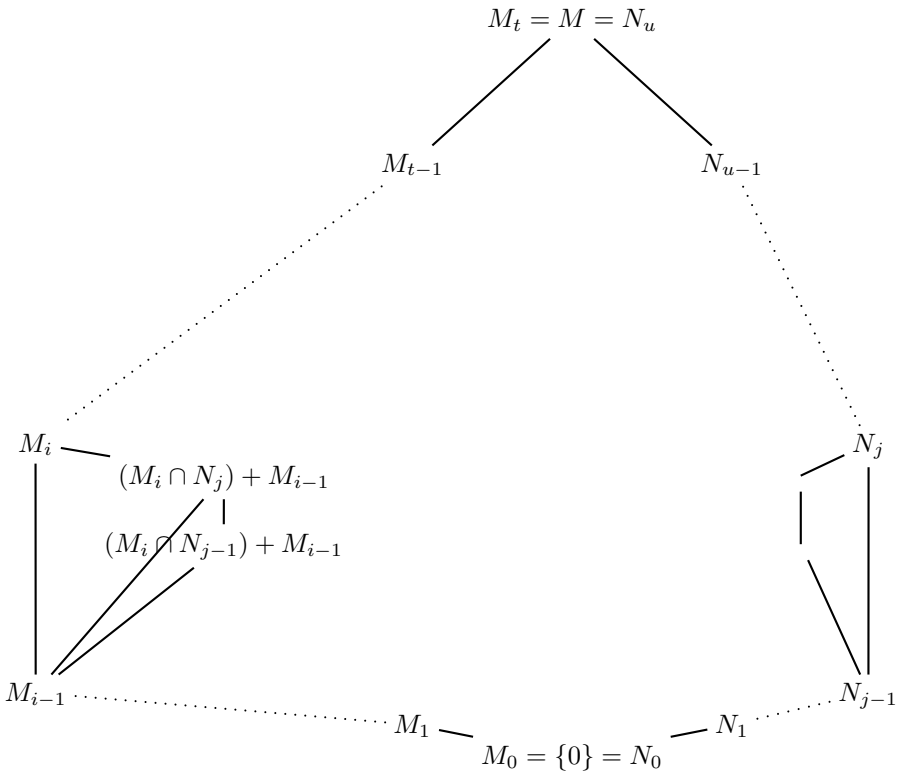
Definition 7.3 (Jordan-Hölder isomorphic)**.** Two modules M and N are *Jordan-Hölder isomorphic* (or *J.-H. isomorphic*) if they have isomorphic chains. We denote this isomorphism by $M \cong_{JH} N$.

We may wonder whether Jordan-Hölder-isomorphism is an equivalent relation. It is easy to see that it is reflexive and symmetric. The problem is to prove that it is transitive. Suppose that a module M is J.-H. isomorphic to N and to L. This means that there are a chain for M and a chain for N which are isomorphic and there are also a chain for M and a chain for L which are isomorphic. Since the two chains for M are not necessarily equal, it is not immediately clear whether N and L also have isomorphic chains.

Definition 7.4 (Refinement)**.** A chain $(M_i)_{i=0}^t$ for M is a *refinement* of a chain $(M_i')_{i=0}^{t'}$ for M if every submodule of M occurs among the M_i at least as often as among the M_i'.

Theorem 7.5 (Schreier refinement theorem)**.** *Every two chains for M have isomorphic refinements.*

Proof. Suppose that we have two chains $(M_i)_{i=0}^t$ and $(N_j)_{j=0}^u$ for M. Then we can refine the chains in the following way.

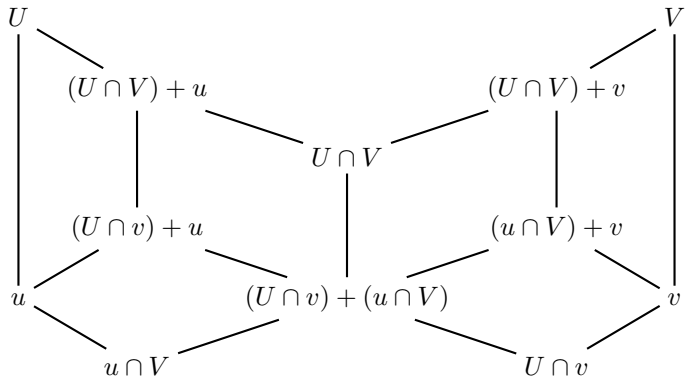


Both chains have length ut and are isomorphic. This follow from the butterfly lemma by Zassenhaus. □

Lemma 7.6 (Butterfly lemma by Zassenhaus)**.** *Let u, U, v, and V be submodules of M with $u \subset U$ and $v \subset V$. Then*

$$((U \cap V) + u)/((U \cap v) + u) \cong_R ((U \cap V) + v)/((u \cap V) + v).$$

Proof. The proof is based on the following diagram, which gives the name to the lemma.



The map $(U \cap V)/((U \cap v) + (u \cap V)) \to ((U \cap V) + u)/((U \cap v) + u)$ is an isomorphism. The kernel consists of all $x + y \in U \cap V$ with $x \in U \cap v$ and $y \in u \cap V$. From the symmetry we see that $(U \cap V)/((V \cap u) + (v \cap U)) \to ((U \cap V) + v)/((V \cap u) + v)$ is also an isomorphism and we are done. □

We also have a refinement theorem for groups, but we need some slight modifications. We require that in a chain

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_t = G$$

every subgroups G_{i-1} is normal in G_i and that in the formulation of the butterfly lemma $u \subset U$ and $v \subset V$ are also normal. The proof becomes longer, because we also have to prove the normality.

Now we can give the answer to the question whether Jordan-Hölder isomorphism is an equivalence relation.

Lemma 7.7. *Jordan-Hölder isomorphism is an equivalence relation.*

Proof. We have already seen that we only need to prove that Jordan-Hölder isomorphism is transitive. Suppose that L and M J.-H. isomorphic and that the chains $(M_i)_{i=0}^t$ for M and $(L_i)_{i=0}^t$ are isomorphic. Moreover, suppose that M is also J.-H. isomorphic to N and let $(M'_j)_{j=0}^u$ for M and $(N_j)_{j=0}^u$ for N be isomorphic chains. We are going to refine the two chains for M following the method in Schreier refinement theorem. We can use any refinement of the chain $(M_i)_{i=0}^t$ in order to refine the chain $(L_i)_{i=0}^t$ in such a way that the refinement of the first chain is isomorphic to the refinement of the second one. Analogously, we can refine the chains $(M'_j)_{j=0}^u$ and $(N_j)_{j=0}^u$. Finally, we find a chain for M which is a refinement of both $(M_i)_{i=0}^t$ and $(M'_j)_{j=0}^u$ and is isomorphic to a refinement of $(L_i)_{i=0}^t$ and to a refinement of $(N_j)_{j=0}^u$. Therefore L and N are J.-H. isomorphic. □

Definition 7.8 (Simple module)**.** A module M is a *simple module* or *irreducible module* if the number of submodules of M is exactly two.

Note that this means that the only submodules of M are $\{0\}$ and M and that M is not equal to $\{0\}$.

Definition 7.9 (Composition series)**.** A chain $(M_i)_{i=0}^t$ of M is a *composition series* if for every $i \in \{1, 2, \ldots, t\}$ the quotient M_i/M_{i-1} is simple.

Since a simple module is different from 0, a composition series may be refined only by repeating submodules.

Definition 7.10. A chain $(M_i)_{i=0}^t$ for M is *echt* if for every $i \in \{1, 2, \ldots, t\}$ it holds that $M_i \neq M_{i-1}$.

Lemma 7.11. *If $(M_i)_{i=0}^t$ and $(N_j)_{j=0}^u$ are two proper chains for M, then each of them has a refinement such that these two refinements are isomorphic and are still proper chains.*

Proof. By Schreier refinement theorem we can refine both chains and find isomorphic refinements

$$0 = M'_0 \subset M'_1 \subset \ldots \subset M'_s = M$$

and

$$0 = N'_0 \subset N'_1 \subset \ldots \subset N'_s = N.$$

Since these refinements are isomorphic, every quotient appears the same number of times. If we remove all the duplicates, we get two isomorphic proper chains. □

Lemma 7.12. *Let $(M_i)_{i=0}^t$ be a chain for M. Then the following are equivalent facts.*

1. *$(M_1)_{i=0}^t$ is composition series.*
2. *Foe every $i \in \{1, 2, \ldots, t\}$ the quotient M_i/M_{i-1} is simple.*
3. *The chain is proper and its unique refinement which is proper is the chain itself.*

Proof. Firstly, we proove that $1 \Rightarrow 2 \Rightarrow 3$. By definition we have $1 \Rightarrow 2$. From 1 it is clear that the chain is proper. Now suppose that there is a refinement of the chain which is proper, but not equal to the chain itself. Hence, there are an i and a module M' such that $M_{i-1} \subsetneq M' \subsetneq M_i$. We get $0 \subsetneq M'/M_{i-1} \subsetneq M_i/M_{i-1}$ and this is a contradiction, because all quotients M_i/M_{i-1} are simple.

For the implication $3 \Rightarrow 1$ we may use the same argument in the other direction. Indeed, if $(M_i)_{i=0}^t$ is a composition series, there exists a quotient M_i/M_{i-1} which is not simple and it therefore contains a proper submodule M'/M_{i-1}. Adding M' to the chain $(M_i)_{i=0}^t$ we obtain a refinement which is a proper chain. □

Any two composition series of M are isomorphic and hence they have the same length.

Now we consider $\mathbb{Z}$-modules, that is abelian groups.

Example.

$$0 \subset 30\mathbb{Z}/60\mathbb{Z} \subset 6\mathbb{Z}/60\mathbb{Z} \subset 2\mathbb{Z}/60\mathbb{Z} \subset \mathbb{Z}/60\mathbb{Z}$$

All simple $\mathbb{Z}$-modules are isomorphic to $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number. These are the only simple abelian groups.

Let A be a $\mathbb{Z}$-module. Then the following are equivalent facts.

1. A has a composition chain.
2. A is finite.

The existence of a composition series

$$0 = A_0 \subset A_1 \subset \ldots \subset A_t = A$$

implies the simplicity of all quotients A_i/A_{i-1}. Hence, every quotient is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number and A is finite.

If A is finite, we may use the next result to prove that A has a composition series.

Definition 7.13 (Finite length)**.** A module M has *finite length* if it has a composition series.

The following are equivalent facts.

1. M has finite length.
2. There exists an integer number b such that any proper chain for M has length less than b.

If any proper chain for M has length less than b, then the refinement of $(M_i)_{i=1}^t$ stops and we find a composition series. The other implication follows by taking b equal to the length of a composition series plus one.

Definition 7.14 (Length)**.** Let $(M_i)_{i=0}^t$ be a composition series of M. Then t is the *length* of M. We will denote the length of M by length(M) or $l(M)$.

Definition 7.15 (S-length and composition factor)**.** Let S be a simple R-module and let M be an R-module of finite length with composition series $(M_i)_{i=0}^{l(M)}$. Then $\#\{i : 0 < i \leq l(M), M_i/M_{i-1} \cong_R S\}$ is the *S-length* of M. We will denote the S-length of M by $l_S(M)$ and we will say that S is a *composition factor* if $l_S(M) \geq 1$.

It is clear that we have

$$l(M) = \sum_{S \text{ (up to isomorphism)}} l_S(M).$$

Example. Consider that case $R = \mathbb{Z}$. The above claim says that if A is a finite abelian group, then

$$\#A = \prod_{p \text{ prime}} p^{l_{\mathbb{Z}/p\mathbb{Z}}(A)}.$$

In other words, if

$$0 = A_0 \subset A_1 \subset \ldots \subset A_t = A$$

is a composition series, then $\#A = \prod_{i=1}^t \#(A_i/A_{i-1})$.

Definition 7.16 (Semisimplification)**.** Let M be an R-module of finite length with composition series $(M_i)_{i=0}^{l(M)}$. 'The' *semisimplification* M_{ss} of M is the R-module

$$M_{\text{ss}} = \bigoplus_{i=1}^{l(M)} (M_i/M_{i-1}).$$

The semisimplication of M is independent of the choice of the composition series. We will see that the semisimplification of M is semisimple, as the name suggests.

Lemma 7.17. *Let L and M be R-modules and let L be simple. Then any R-homomorphism $f : L \to M$ is either the zero homomorphism or injective and any R-homomorphism $g : M \to L$ is either the zero homomorphism or surjective.*

Proof. We know that $\ker f$ is a submodule of L and hence either $\ker f = L$ or $\ker f = 0$. In the first case $f \equiv 0$, in the second one f is injective.

Since $g(M)$ is a submodule of L, either $g(M) = 0$ or $g(M) = L$. In the former case $g \equiv 0$, in latter one g is surjective. □

The following are consequences of the previous lemma.

1. If L and L' are simple, then any R-linear map $L \to L'$ is either the zero map or an isomorphism.
2. If L is simple, then $\mathrm{End}_R(L)$ is a division ring ("Schur's lemma"). For instance, if $L = \mathbb{Z}/p\mathbb{Z}$, then $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{F}_p$.
3. If L and L' are two simple R-modules and they are not isomorphic, then $\mathrm{Hom}_R(L, L') = 0$.

Definition 7.18 (Maximal ideal)**.** A *maximal ideal* of a commutative ring R is an ideal $\mathfrak{m} \subset R$ of R such that $\#\{I : I \text{ ideal of R}, \mathfrak{m} \subset I \subset R\} = 2$.

An equivalent definition is that an ideal $\mathfrak{m} \subset R$ is maximal if and only if $R/\mathfrak{m}$ is simple.

By Zorn's lemma, every commutative ring which is not equal to 0 has a maximal ideal. It is important that $1 \in R$.

If a simple module L over a commutative ring R is isomorphic to $R/\mathfrak{m}$, then

$$\begin{array}{rcl} \mathfrak{m} = \ker(R & \overset{\text{ring homomorphism}}{\longrightarrow} & \mathrm{End}_{\mathbb{Z}}(L)) \\ (r & \longmapsto & (x \mapsto rx)). \end{array}$$

Thus, $R/\mathfrak{m} \cong_R R/\mathfrak{m}' \Rightarrow \mathfrak{m} = \mathfrak{m}'$.

Let R be a ring, not necessarily commutative.

Definition 7.19 (Maximal left ideal)**.** A left ideal I of R is a *maximal left ideal* if $\#\{J : J \text{ is a left ideal of } R, I \subset J \subset R\} = 2$.

An equivalent definition is that a left ideal I of R is maximal if and only if R/I is simple as an R-module.

By Zorn's lemma, every ring different from 0 has a maximal left ideal.

Theorem 7.20. *Every simple R-module is of the form R/I where I is a maximal left ideal.*

Proof. Suppose L is simple and choose $x \in L \setminus \{0\}$. Map R onto L as follows.

$$\begin{array}{rcl} g : R & \longrightarrow & L \\ r & \longmapsto & rx. \end{array}$$

The map g is R-linear and $g \not\equiv 0$. By Lemma 7.17, g is surjective. Hence, $L \cong_R R/\ker g$ where $\ker g$ is a maximal left ideal, because $R/\ker g$ is simple. □

Let k be a field n be a natural number greater than 1. We take $R = \mathrm{M}(n, k) = \{n \times n - \text{matrices with coefficients in } k\}$ and $L = k^n$, where we consider k^n as the set of column vectors of n elements of k. Then L is an R-module via $A \cdot v \in L$ for $A \in R$ and $v \in L$.

Now we are going to prove that L is simple. Suppose that M is a submodule such that $0 \subsetneq M \subsetneq L$. Let v be a nonzero element of M. It is a well-known fact from linear algebra that, if $v, w \in k^n$ with $v \neq 0$, there is a linear transformation $k^n \to k^n$ such that $v \mapsto w$. Thus, for all $w \in L$ there exists $A \in R$ such that $Av = w$.

We look for a maximal left ideal $I \subset M(n, k) = R$ with $R/I \cong_R L$. Choose

$$x = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in L = k^n.$$

We can take

$$I = \left\{ A \in R : A \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right\}$$
$$= \left\{ \begin{pmatrix} 0 & * & * & * & * \\ 0 & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & * & * & * & * \end{pmatrix} \in R \right\}.$$

Changing x (take also

$$x = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ etc.)}$$

we find n left ideals I such that $R/I \cong_R L$.

Theorem 7.21. *Let R be a ring and M be an R-module of finite length. Then M is finitely generated.*

Proof. The proof is by induction on $l(M)$. If $l(M) = 0$, then M is 0 and we are done. If $l(M) = t > 0$, then consider the composition series $0 = M_0 \subset M_1 \subset \ldots \subset M_t = M$. By inductive hypothesis, M_{t-1} is finitely generated. The quotient M_t/M_{t-1} is simple, hence M_t/M_{t-1} is isomorphic to $R/$(maximal left ideal) and is generated by one element $x + M_{t-1}$. The module M is generated by M_{t-1} and x, therefore it is finitely generated. □

The previous proof also shows that the number of generators is bounded by $l(M)$.

Theorem 7.22. *Let M be an R-module and $N \subset M$ be a submodule. Then the following are equivalent facts.*

1. *The module M has finite length.*
2. *Both N and M/N have finite length.*

In other words, for every short exact sequence $0 \to N \to M \to L \to 0$ the module M has finite length if and only if both N and L have finite length. Moreover, the above statements imply that $l(M) = l(N)+l(M/N)$ and that for every simple R-module S we have $l_S(M) = l_S(N)+l_S(M/N)$.

Proof. 1 ⇒ 2. We have $0 \subset N \subset M$. If N has proper chains of arbitrary length, then M also has such chains. If we quotient the above chain by N, we find $0 \subset M/N$, where N is mapped to 0 and M is mapped surjectively onto M/N. Thus, if M/N has proper chains of arbitrary length, then M also has such chains.

2 ⇒ 1 and the last implication. Let $0 = N_0 \subset N_1 \subset \ldots \subset N_u = N$ and $0 = L_0 \subset L_1 \subset \ldots \subset L_v = M/N$ be composition series. Let f be the projection map $M \to M/N$, which is clearly surjective. Thus, $0 = N_0 \subset N_1 \subset \ldots \subset N_u = N = f^{-1}L_0 \subset f^{-1}L_1 \subset f^{-1}L_v = M$ is a composition series of M and $l(M) = u + v = l(N) + l(M/N)$. Since all quotients do not change, we also have $l_S(M) = l_S(N) + l_S(M/N)$. □

Chapter 8

Additive invariants

Let R be a ring and let $\mathcal{C}$ be a class of R-modules with $0 \in \mathcal{C}$.
Examples.
$\mathcal{C} = \{\text{all } R\text{-modules}\}$
$\mathcal{C} = \{\text{all finetely generated } R\text{-modules}\}$
$\mathcal{C} = \{\text{all } R\text{-modules of finite length}\}$

Definition 8.1 (Additive function)**.** Let A be an abelian group. A function $f : \mathcal{C} \to A$ is an *additive function* if for every exact sequence $0 \to N \to M \to L \to 0$ with L, M, $N \in \mathcal{C}$ it holds that $f(M) = f(N) + f(L)$. We also call f an *additive invariant*.

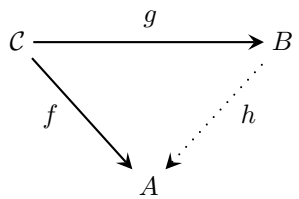
If we take $N = M = L = 0$ in the definition, we find that $f(0) = 0$ for every additive invariant f. If we choose $L = 0$, then $N \cong M$ implies $f(M) = f(N)$.
Example. $R = \mathbb{Z}$, $\mathcal{C} = \{\text{finite abelian groups}\}$, $A = \mathbb{Q}^*_{>0}$, $f(M) = \#M$.
We denote the set of additive functions $\mathcal{C} \to A$ by $\mathrm{Add}(\mathcal{C}, A)$.

Definition 8.2 (Universal additive function)**.** Let B be an abelian group. A function $g : \mathcal{C} \to B$ is a *universal additive function* if g is additive and for every abelian group A the map

$$\begin{array}{ccc} \mathrm{Hom}(B, A) & \longrightarrow & \mathrm{Add}(\mathcal{C}, A) \\ h & \longmapsto & hg \end{array}$$

is a bijection.

In other words, g is universal additive if g is additive and for every abelian group A and for every additive $f : \mathcal{C} \to A$ there exists a unique group homomorphism $h : B \to A$ which make the following diagram commute.



Now we want to construct a universal additive function given R and $\mathcal{C}$. Let $\mathbb{Z}^{(\mathcal{C})} = \{(n_M)_{M \in \mathcal{C}} : n_M \in \mathbb{Z}, \#\{M : n_M \neq 0\} < \infty\}$. For every $M \in \mathcal{C}$ we define a vector $e_M \in \mathbb{Z}^{(\mathcal{C})}$ as follows.

The vector e_M has a 1 at position M and 0 at all other positions. The e_M are basis vectors of $\mathbb{Z}^{(\mathcal{C})}$. We may also write $(n_M)_{M\in\mathcal{C}} = \sum_M^{<\infty} n_M e_M$. Let H be the subgroup generated by $\{e_M - e_L - e_N : 0 \to L \to M \to N \to 0 \text{ is a short exact sequence in } \mathcal{C}\}$. In $\mathbb{Z}^{(\mathcal{C})}/H$ we have $\overline{e_M} = \overline{e_L} + \overline{e_N}$. We denote $\mathbb{Z}^{(\mathcal{C})}/H$ by $K(\mathcal{C})$.

Definition 8.3 (Grothendieck group)**.** The group $K(\mathcal{C})$ is called the *Grothendieck group* of $\mathcal{C}$.

For every $M \in \mathcal{C}$ we will denote the element $\overline{e_M}$ of $K(\mathcal{C})$ by $[M]$.

Definition 8.4 (Effective and virtual elements)**.** An element of $K(\mathcal{C})$ is *effective* if it is of the form $[M]$ with $M \in \mathcal{C}$. Other elements are *virtual*.

Theorem 8.5. *The function $\mathcal{C} \xrightarrow{[\,]} K(\mathcal{C})$ is universal additive.*

Proof. Let A be an abelian group. Note that $\mathrm{Hom}(\mathbb{Z}^{(\mathcal{C})}, A) = \{\text{all functions } \mathcal{C} \to A\}$. Then

$$\begin{aligned}\mathrm{Hom}(K(\mathcal{C}), A) &= \mathrm{Hom}(\mathbb{Z}^{(\mathcal{C})}/H, A) \cong \{j \in \mathrm{Hom}(\mathbb{Z}^{(\mathcal{C})}, A) : j|_H = 0\}\\ &\cong \{f : \mathcal{C} \to A : \forall 0 \to N \to M \to L \to 0 : f(M) = f(L) = f(N)\}\\ &= \mathrm{Add}(\mathcal{C}, A).\end{aligned}$$

□

Lemma 8.6. *If $\mathcal{C}$ is closed under $\oplus$, then every element of $K(\mathcal{C})$ is of the form $[M] - [M']$ with $M, M' \in \mathcal{C}$.*

Proof. It is clear that $\{[M] : M \in \mathcal{C}\}$ generates the group $K(\mathcal{C})$. For $M, M', N, N' \in \mathcal{C}$ we have $([M] - [M']) - ([N] - [N']) = [M] + [N'] - ([M'] + [N]) = [M \oplus N'] - [M' \oplus N]$, because the sequences $0 \to M \to M \oplus N' \to N' \to 0$ and $0 \to M' \to M' \oplus N \to N \to 0$ are exact. Hence, the subset $\{[M] - [M'] : M, M' \in \mathcal{C}\}$ is a subgroup of $K(\mathcal{C})$ which contains all generators and therefore $\{[M] - [M'] : M, M' \in \mathcal{C}\} = K(\mathcal{C})$. □

Example. Let R be a ring.

1. If $\mathcal{C} = \{\text{all } R\text{-modules}\}$, then $K(\mathcal{C}) = 0$.

   Proof. Consider the following exact sequence

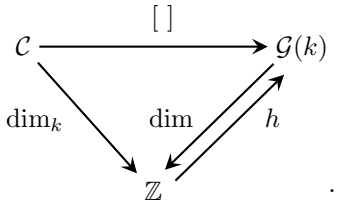
   $$0 \to M \xrightarrow{f} \bigoplus_{i=0}^{\infty} M \xrightarrow{g} \bigoplus_{i=0}^{\infty} M \to 0,$$

   with $f(x) = (x, 0, \ldots, 0)$ and $g(x_0, x_1, x_2, \ldots) = (x_1, x_2, \ldots)$. Then $[\bigoplus_{i=0}^{\infty} M] = [M] + [\bigoplus_{i=0}^{\infty} M]$, thus $[M] = 0$. □

2. Let $\mathcal{C} = \{\text{finitely generated } R\text{-modules}\}$. Notation: $K(\mathcal{C}) = \mathcal{G}(R) = \mathcal{G}_{\mathrm{fg}}(R)$.

   Theorem 8.7. *Let k be a field. Then $\dim : \mathcal{G}(k) \xrightarrow{\sim} \mathbb{Z}$ is an isomorphism.*

   Proof. Let $\mathcal{C} = \{\text{finitely generated } k\text{-modules}\} = \{\text{finite-dimensional } k\text{-vector spaces}\}$. Then we have the following diagram.



We have the map $\dim : \mathcal{G}(k) \to \mathbb{Z}$ and it is unique because of the universality of $[\ ]$ by Theorem 8.5). This map is given by $[M] \longmapsto \dim_k(M)$ and it is well-defined, because $M \cong N \Leftrightarrow \dim_k(M) = \dim_k(N)$. We will show that is also bijective by proving that the map $n \mapsto n[k]$ is the inverse of dim. We have $[k^a] + [k^b] = [k^{a+b}]$ and by induction we get $n[k] = [k^n]$. Now let $M \in \mathcal{C}$ with $\dim_k(M) = n$ and note that $M \cong k^n$ and $[M] = [k^n]$. Thus, $n \overset{h}{\longmapsto} n[k] = [k^n] = [M] \overset{\dim}{\longmapsto} n$ and $[M] \overset{\dim}{\longmapsto} \dim_k(M) = n \overset{h}{\longmapsto} [k^n] = [M]$. □

We also have $\mathcal{G}(\mathbb{Z}) \cong \mathbb{Z}$.

Proof. Every finite abelian group is isomorphic to a product of cyclic groups $\bigoplus_{i=1}^{r}(\mathbb{Z}/n_i\mathbb{Z})$ where $n_i \in \mathbb{Z}_{\geq 0}$.

For $n \in \mathbb{Z}_{>0}$ we have the exact sequence $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$. Thus, $[\mathbb{Z}/n\mathbb{Z}] = 0$. Now we get the isomorphism

$$[M] = \left[\bigoplus_{i=1}^{r}(\mathbb{Z}/n_i\mathbb{Z})\right] \longmapsto \#\{i : 1 \leq i \leq r, n_i = 0\} = \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} M)$$

and we are done. □

3. Let $\mathcal{C} = \{\text{all } R\text{-modules of finite length}\}$. We write $K(\mathcal{C})$ as $\mathcal{G}_{\mathrm{fl}}(R)$.

Theorem 8.8. *There exists a group isomorphism*

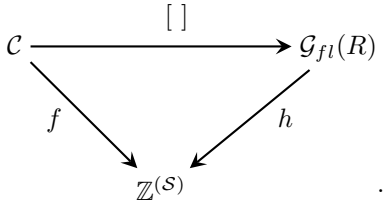
$$\begin{array}{rcl} \mathcal{G}_{fl}(R) & \xrightarrow{\sim} & \mathbb{Z}^{(\mathcal{S})} \\ [M] & \longmapsto & (l_S(M))_{S \in \mathcal{S}}, \end{array}$$

where $\mathcal{S} = \{\textit{simple } R\textit{-modules}\}/\cong_R$.

Proof. Since for every $S \in \mathcal{S}$ we have $l_S(M) = l_S(N) + l_S(L)$ if the sequence $0 \to L \to M \to N \to 0$ is exact, the function

$$\begin{array}{rcl} f : \mathcal{C} & \longrightarrow & \mathbb{Z} \\ M & \longmapsto & (l_S(M))_{S \in \mathcal{S}} \end{array}$$

is additive invariant. The universal property of $\mathcal{G}_{fl}(R)$ gives a map $h : \mathcal{G}_{fl}(R) \to \mathbb{Z}^{(\mathcal{S})}$ and the following commutative diagram.



We will show that the map

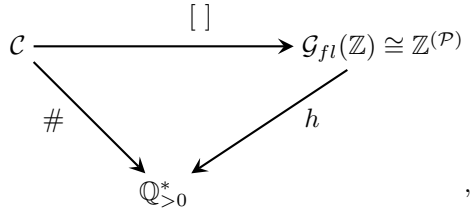
$$\begin{array}{rcl} j : \mathbb{Z}^{(\mathcal{S})} & \longrightarrow & \mathcal{G}_{fl}(R) \\ (n_S)_{S\in\mathcal{S}} & \longmapsto & \sum_{S\in\mathcal{S}} (n_S[S]) \end{array}$$

is the inverse of h. Firstly, the map j is a left inverse , because $hj[e_S] = h([S]) = e_S$. Conversely, $jh([M]) = j(\sum_{S\in\mathcal{S}} l_S(M)e_S) = \sum_{S\in\mathcal{S}} l_S(M)[S] = \sum_{i=1}^{t}[M_i/M_{i-1}]$, if $0 = M_0 \subset M_1 \subset \ldots \subset M_t = M$ is composition series of M.

For $1 \leq u \leq t$ the sequence $0 \to M_{u-1} \to M_u \to M_u/M_{u-1} \to 0$ is exact. Thus, we have $[M_u] = [M_{u-1}] + [M_u/M_{u-1}]$. By induction on u we get $\sum_{i=1}^{t}[M_i/M_{i-1}] = [M]$. This proves that the map j is a left inverse of h. □

Note that under this isomorphism the subgroup of effective elements of $\mathcal{G}_{fl}(R)$ has image $\mathbb{Z}_{\geq 0}^{(\mathcal{S})}$.

Example. Let $R = \mathbb{Z}$ and $\mathcal{C} = \{\text{finite abelian groups}\}$. Let $\mathcal{P}$ be the set of prime numbers $\{2, 3, 5, \ldots\}$. Then we have the following commutative diagram.



,

where the map h given by $(n_p)_{p\in\mathcal{P}} \mapsto \prod_{p\in\mathcal{P}} p^{n_p}$ is an isomorphism, because of the unique prime factorization.

Corollary 8.9. *Let M and N be R-modules of finite length. Then*

$$\begin{array}{rcl} [M] = [N] & \Leftrightarrow & \textit{both } M \textit{ and } N \textit{ have isomorphic composition chains} \\ & \Leftrightarrow & M \cong_{JH} N \\ & \Leftrightarrow & M_{\text{ss}} \cong N_{\text{ss}}. \end{array}$$

Example. Let $G = \langle\sigma\rangle$ with $\#G = 2$ and let k be a field of characteristic different from 2. We have seen that every $k[G]$-module V is of the form $V_+ \oplus V_-$, where both V_+ and V_- are k-vector spaces such that for all $x \in V_+ : \sigma x = x$ and for all $x \in V_- : \sigma x = -x$.

If V is simple, then we have either $V = V_+$ or $V = V_-$.

Moreover, for every nonzero element $v \in V$ we see that kv is a nontrivial $k[G]$-submodule of V. Hence, if V is simple, we have $\dim V = 1$.

Therefore, V is simple if and only if (either $V = V_+$ or $V = V_-$) and $\dim V = 1$.

In conclusion, every simple $k[G]$-module is isomorphic either to k_+ or to k_-, where $k_+ := k$ with $\sigma x = x$ for all $x \in k_+$ and $k_- := k$ with $\sigma x = -x$ for all $x \in k_-$. We leave to the reader the proof that k_+ and k_- are non-isomorphic $k[G]$-modules.

Theorem 8.8 gives the following isomorphism.

$$\begin{array}{rcl} \mathcal{G}_{\text{fl}}(k[G]) & \xrightarrow{\sim} & \mathbb{Z} \oplus \mathbb{Z} \\ [V] & \longmapsto & (\dim_k V_+, \dim_k V_-). \end{array}$$

Note that V has finite length over $k[G] \Leftrightarrow \dim_k V < \infty \Leftrightarrow \dim_k V_+ < \infty$ and $\dim_k V_- < \infty$.

Theorem 8.10. *Let k be a field and R be a ring which contains k as a subring and suppose that $k \subset Z(R)$ and $\dim_k R < \infty$. Let M be an R-module. Then the following facts are equivalent.*

1. *M is finitely generated as R-module;*
2. *M has finite length as R-module;*
3. *$\dim_k M < \infty$.*

Furthermore, $1 \leq \#\mathcal{S} < \infty$, where $\mathcal{S} = \{\text{simple } R\text{-modules}\}/\cong_R$.

Example of rings R which satisfy the previous conditions are k, finite field extensions of k, group rings $k[G]$ with G a finite group, and matrix rings $\mathrm{M}(n,k)$.

Proof. We have already proven that $(ii) \Rightarrow (i)$.

$(i) \Rightarrow (iii)$. The module M is finitely generated. Thus, there exists a natural number n such that R^n maps surjectively onto M. This implies that $\dim_k(M) \leq \dim_k(R^n) = n \dim_k(R) < \infty$.

$(iii) \Rightarrow (ii)$. Every R-submodule of M is also a k-submodule. Hence, every R-chain of M is also a k-chain and the length of every proper R-chain is not larger than the length of a maximal proper k-chain. This is equal to $\dim_k M$.

Note that this proof also show that $\mathrm{length}_R(M) \leq \dim_k(M)$.

Proof of $1 \leq \#\mathcal{S} < \infty$. The ring R is a finitely generated R-module. Hence, R has finite length as an R-module. If S is a simple module, then by Theorem 7.20 we have $S = R/L$ where L is a maximal left ideal of R. There exists a composition series of R of the form $0 \subset ... \subset L \subset R$. Hence, $l_S(R) \geq 1$ and

$$l(R) = \sum_{S \in \mathcal{S}} l_S(R) \geq \#\mathcal{S}.$$

Thus, $1 \leq \#\mathcal{S} < \infty$.

Note that the same proof gives that $\#\mathcal{S} \leq l(R) \leq \dim_k(R)$. □

Theorem 8.11. *Let k and R be as in the previous theorem. Let S be a simple R-module. Then the endomorphisms ring $\mathrm{End}_R(S)$ is a division ring, it contains k in its centre and $\dim_k(End_R(S)) < \infty$.*

If k is also algebraically closed, then $\mathrm{End}_R(S) = k$.

Proof. Let f a nonzero element of $\mathrm{End}_R(S)$ Then $\ker(f) = 0$ and $\mathrm{im}(f) = S$, because S is simple and the only submodules are 0 and S. Hence $\mathrm{End}_R(S)$ is a division ring.

Since S is simple, it has finite length and by Theorem 8.10 we get $n := \dim_k(S) < \infty$.

We have $\mathrm{End}_R(S) \subset \mathrm{End}_k(S) \cong \mathrm{M}(n,k)$. It is well-known that $\dim_k(M(n,k)) = n^2 < \infty$. The ring $\mathrm{End}_R(S)$ contains k and, since $k \subset Z(M(n,k))$, then $k \subset Z(\mathrm{End}_R(S))$.

Now suppose that k is algebraically closed. We already know that $k \subset \mathrm{End}_R(S)$. Hence, we only need to prove that $k \supset \mathrm{End}_R(S)$.

Choose $\alpha \in \mathrm{End}_R(S)$ and define the ring homomorphism

$$\begin{array}{rcl} \varphi : k[X] & \longrightarrow & \mathrm{End}_R(S) \\ \sum a_i X^i & \longmapsto & \sum a_i \alpha^i. \end{array}$$

Since $k[X]$ is commutative and $\mathrm{End}_R(S)$ is a division ring, the image of φ is a domain. Therefore, the kernel $\ker\varphi$ is a prime ideal of $k[X]$, that is $\ker\varphi = (X-a)$ with $a \in k$. Note that $\ker\varphi \neq 0$, because $\dim_k(\mathrm{End}_R(S)) < \infty$ and $\dim_k(k[X]) = \infty$.

Now $\varphi(X-a) = 0 = \alpha - a$. Hence, $\alpha = a$. □

Let k be a field, G be a finite group and $R = k[G]$. We denote by $\mathcal{R}(G) = \mathcal{R}_k(G) = \mathcal{G}(k[G])$ the Grothendieck group of the $k[G]$-modules of finite k-dimension.

Theorem 8.12. *Let k be a field and G be a finite group. Then $\mathcal{R}_k(G)$ has a unique ring via the given addition and the multiplication such that $[M][N] = [M \otimes_k N]$ for any two finitely generated $k[G]$-modules M and N. $M \otimes_k N$ is a $k[G]$-module via $\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y)$ for all $\sigma \in G$, $x \in M$, $y \in N$. The ring is commutative.*

Example. If $\#G = 2$ and k is a field of characteristic different from 2, then $\mathcal{S} = \{k_+, k_-\}$ and $\mathcal{R}(G) = \mathbb{Z}[k_+] \oplus \mathbb{Z}[k_-]$.

Let $\epsilon, \eta \in \{\pm 1\}$. We know that $k_\epsilon \otimes_k k_\eta = k$ as k-vector spaces. For all $x \in k_\epsilon$, $y \in k_\eta$ we have $\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y) = \epsilon x \otimes \eta y = \epsilon\eta(x \otimes y)$. Hence, $[k_\epsilon][k_\eta] = [k_{\epsilon\eta}]$ and $\mathcal{R}(G) \cong \mathbb{Z}[\text{group of order 2}]$ as rings.

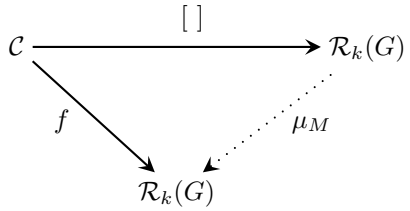
Proof. We have to define a multiplication $\mathcal{R}_k(G) \times \mathcal{R}_k(G) \longrightarrow \mathcal{R}_k(G)$ which satisfies the properties of the theorem.

Firstly, fix M and consider the map

$$\begin{array}{rcl} f : \mathcal{C} & \longrightarrow & \mathcal{R}_k(G) \\ N & \longmapsto & [M \otimes_k N]. \end{array}$$

If the sequence $0 \to N_1 \to N_2 \to N_3 \to 0$ is exact, then the sequence $M \otimes_k N_1 \to M \otimes_k N_2 \to M \otimes_k N_3 \to 0$ is also exact. Since k is a field, the first sequence splits as a sequence of k-modules. It follows that the induced map $M \otimes_k N_1 \to M \otimes_k N_2$ is injective. Thus, $0 \to M \otimes_k N_1 \to M \otimes_k N_2 \to M \otimes_k N_3 \to 0$ is exact. Since all maps are also $k[G]$-linear, the function f is an additive invariant.

The universal property of $\mathcal{R}_k(G)$ gives a unique group homomorphism μ_M such that $\mu_M([N]) = [M \otimes_k N]$.

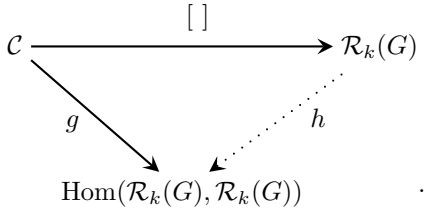


Now consider the map

$$\begin{array}{rcl} g : \mathcal{C} & \longrightarrow & \mathrm{Hom}(\mathcal{R}_k(G), \mathcal{R}_k(G)) \\ M & \longmapsto & \mu_M. \end{array}$$

Check that this map is also an additive invariant. The proof is almost the same as the previous one.

The universality gives a unique group homomorphism $h : \mathcal{R}_k(G) \longrightarrow \mathrm{Hom}(\mathcal{R}_k(G), \mathcal{R}_k(G))$ such that the following diagram commutes.



Define the multiplication in $\mathcal{R}_k(G)$ by $xy = h(x)(y)$ for all $x, y \in \mathcal{R}_k(G)$.

By construction this map has the desired property $[M][N] = [M \otimes_k N]$, because $[M][N] = h([M])[N] = \mu_M([N]) = [M \otimes_k N]$.

Distributive laws follow from bilinearity. Associativity follows from $(L \otimes_k M) \otimes_k N \cong_{k[G]} L \otimes_k (M \otimes_k N)$.

The element $[k]$ associated to the $k[G]$-module k with $\sigma x = x$ for all $\sigma \in G$, $x \in k$ acts as the unit element. Check that the map $k \otimes_k N \to N$ with $x \otimes y \mapsto xy$ gives a $k[G]$-linear isomorphism.

Commutativity of the multiplication follows from the commutativity of $- \otimes_k -$. □

Theorem 8.13. *Let k be a field and G be a finite group. Then $\mathcal{R}_k(G)$ has a unique ring automorphism $\overline{\ }$ where for every finitely generated $k[G]$-module M it holds that $\overline{[M]} = [\mathrm{Hom}_k(M, k)]$. The module $\mathrm{Hom}_k(M, k)$ is a $k[G]$-module via $\sigma f(m) = f(\sigma^{-1}m)$ for all $\sigma \in G$, $f \in \mathrm{Hom}_k(M, k)$, $m \in M$. This ring automorphism is an involution.*

Note that this G-action on $\mathrm{Hom}_k(M, k)$ is obtained as follows. It is known that $\mathrm{Hom}_k(M, k)$ is a right $k[G]$-module. Hence, it is a left $k[G]^{\mathrm{opp}}$-module. The ring isomorphism

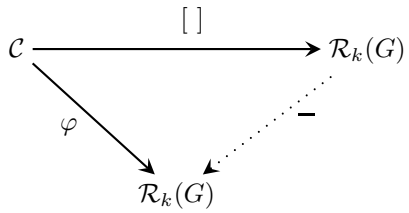
$$\begin{array}{rcl} k[G] & \longrightarrow & k[G]^{\mathrm{opp}} \\ \sum a_\sigma \sigma & \longmapsto & \sum a_\sigma \sigma^{-1} \end{array}$$

makes $\mathrm{Hom}_k(M, k)$ a left $k[G]$-module.

Proof. We use the notation $M^\dagger := \mathrm{Hom}(M, k)$.

Suppose that $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of finitely generated $k[G]$-modules. Because as a sequence of k-modules it splits and $\mathrm{Hom}_k(M, k)$ is left exact, we see that $0 \to M_3^\dagger \to M_2^\dagger \to M_3^\dagger \to 0$ is also an exact sequence of $k[G]$-linear maps. Thus, $[M_2^\dagger] = [M_1^\dagger] + [M_3^\dagger]$ and $\varphi : M \to [M^\dagger]$ is an additive invariant.

From the universal property we get a unique *group isomorphism* $\overline{\ }: \mathcal{R}_k(G) \to \mathcal{R}_k(G)$ such that $\forall M \in \mathcal{C} : \overline{[M]} = [M^\dagger]$.



The map

$$\begin{array}{rcl} M & \longrightarrow & M^{\dagger\dagger} = \mathrm{Hom}_k(\mathrm{Hom}_k(M, k), k) \\ x & \longmapsto & (f \mapsto f(x)) \end{array}$$

is a $k[G]$-linear isomorphism. Hence, $\overline{\overline{[M]}} = [M]$ and $\overline{\ }$ is its own inverse. In particular, it is a group isomorphism.

To prove that $\overline{\ }$ is also a ring isomorphism, it is sufficient to prove it for generators of $\mathcal{R}_k(G)$. We need to show that $[M^\dagger][N^\dagger] = [(M \otimes_k N)^\dagger]$. We have already seen that $[M^\dagger][N^\dagger] = [M^\dagger \otimes_k N^\dagger]$.

We construct a homomorphism

$$\begin{array}{rcl} \psi_{M,N} : \mathrm{Hom}_k(M, k) \otimes_k \mathrm{Hom}_k(N, k) & \longrightarrow & \mathrm{Hom}_k(M \otimes_k N, k) \\ f \otimes g & \longmapsto & (x \otimes y \mapsto f(x)g(y)). \end{array}$$

The existence of ψ follows from universal properties of the two tensor products we use. Moreover, ψ is a $k[G]$-linear map.

If $M = N = k$, the map $\psi_{M,N}$ is an isomorphism. Now check that $\psi_{M,N}$ is also an isomorphism if both M and N are finite direct sums of k. This proves that $\psi_{M,N}$ is an isomorphism for finite-dimensional vector spaces M and N, and therefore for $M, N \in \mathcal{C}$.

The isomorphism ψ gives an isomorphism between $M^\dagger \otimes_k N^\dagger$ and $(M \otimes_k N)^\dagger$. This proves that $[M^\dagger \otimes_k N^\dagger] = [(M \otimes_k N)^\dagger]$. □

Chapter 9

Semisimplicity

Proposition 9.1. *Let M be a semisimple module.*

- *If $0 \to L \to M \to N \to 0$ is exact, then both L and N are semisimple.*
- *If $M \neq 0$, then M has a simple submodule.*

Proof. Suppose that the sequence $0 \to L \xrightarrow{f} M \to N \to 0$ is exact. Firstly, we show that L is semisimple.

Suppose that the sequence $0 \to J \xrightarrow{h} L \to K \to 0$ is exact. Since both h and f are injective, the composite function $i := fh$ is also injective and we can construct the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \xrightarrow{h} & L & \longrightarrow & K & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_J} & & \downarrow{\scriptstyle f} & & & & \\ 0 & \longrightarrow & J & \xrightarrow{i} & M & \longrightarrow & M/J & \longrightarrow & 0. \end{array}$$

Since M is semisimple, the second row splits and there is an R-linear map $j : M \to J$ such that $ji = \mathrm{id}_J$. Define $k := jf$. Then $kh = jfh = ji = \mathrm{id}_J$, and therefore the first row also splits. Hence, L is semisimple.

Since the sequence $0 \to L \to M \to N \to 0$ splits, we have $M \cong L \oplus N$. Thus, there is also a split sequence $0 \to N \to M \to L \to 0$. It follows that N is also semisimple.

Now choose a nonzero element $x \in M$. Then $Rx \subset M$ is a submodule of R isomorphic to R/I where $I = \mathrm{Ann}(x)$. Note that $I \neq R$. Let L with $I \subset L \subset R$ a maximal left ideal. Then R/L is simple.

Consider the exact sequence $0 \to L/I \to R/I \to R/L \to 0$. This sequence splits, because M is semisimple. Hence, $Rx \cong R/I \subset M$ is also semisimple and we have $(L/I) \oplus (R/L) \cong R/I \cong Rx \subset M$. The module R/L is isomorphic to a simple submodule of M and we are done. □

Theorem 9.2. *Let R be a ring and M be an R-module. The following facts are equivalent.*

1. *M is semisimple.*
2. *There exist a collection $(S_i)_{i \in I}$ of simple R-modules and an isomorphism $M \cong \bigoplus_{i \in I} S_i$.*
3. *There exist a collection $(S_i)_{i \in I}$ of simple R-modules and a surjective R-linear map $\bigoplus_{i \in I} S_i \twoheadrightarrow M$.*

Example. Take $R = \mathbb{Z}$. Then M is semisimple if and only if $M \cong \bigoplus_{i\in I} \mathbb{Z}/p_i\mathbb{Z}$ where the numbers p_i are prime.

Proof. (1) $\Rightarrow$ (3). Take $\mathcal{T} = \{\text{simple submodules of } M\}$ and consider the map

$$\begin{aligned} f : \bigoplus_{S\in\mathcal{T}} S &\longrightarrow M \\ (x_S)_{S\in\mathcal{T}} &\longmapsto \sum_{S\in\mathcal{T}} x_S. \end{aligned}$$

Define N as the image of f. Since M is semisimple, there exist a submodule $K \subset M$ such that $M = N \oplus K$.

If $K = 0$, the map f is the requested surjection. Hence, we may assume that $K \neq 0$. Since K is semisimple, by Proposition 9.1 K has a simple submodule U. We have $U \in \mathcal{T}$, because $U \subset M$. This means that $U \subset N$, which contradicts $N \cap K = 0$.

(3) $\Rightarrow$ (2).

Let $f : \bigoplus_{i\in I} S_i \longrightarrow\!\!\!\!\!\rightarrow M$ as in the theorem.

Define for a subset $J \subset I$ the map $f_J : \bigoplus_{i\in J} S_i \to M$ induced by f.

$$\begin{array}{ccc} \bigoplus_{i\in I} S_i & \xrightarrow{\ f\ } & M \\ \cup & \nearrow_{f_J} & \\ \bigoplus_{i\in J} S_i & & \end{array}$$

By Zorn's lemma, we can choose a maximal subset J from all subsets $J' \subset I$ where $f_{J'}$ is injective. We will prove that f_J is also surjective.

If $I = J$, we are done. Now suppose that $I \neq J$ and let $h \in I \setminus J$. The maximality of J implies that $f_{(J\cup\{h\})}$ is not injective. Hence, the map $S_h \overset{f_{\{h\}}}{\to} M \to M/(\mathrm{im}(f_J))$ is not injective. Since S_h is simple, this map has to be the zero map. This means that the image of S_h is contained in the image of f_J.

Hence, for all $i \in I$ the image of $f_{\{i\}}$ in M is contained in $\mathrm{im}(f_J)$, that is the whole image of f is contained in $\mathrm{im}(f_J)$.

(2) $\Rightarrow$ (1). Suppose that the short sequence $0 \to L \to \bigoplus_{i\in I} S_i \overset{p}{\to} N \to 0$ is exact.

The method in the proof of (3) $\Rightarrow$ (2) gives from the surjection p a subset J and a map p_J such that $p_J : \bigoplus_{i\in J} S_i \to N$ is an isomorphism.

$$\begin{array}{ccc} \bigoplus_{i\in I} S_i & \xrightarrow{\ p\ } & N \\ \cup & \nearrow_{p_J} & \\ \bigoplus_{i\in J} S_i & & \end{array}$$

The homomorphism $N \overset{p_J^{-1}}{\to} \bigoplus_{i\in J} S_i \hookrightarrow \bigoplus_{i\in I} S_i$ gives a splitting of the exact sequence. □

Definition 9.3 (Semisimple ring)**.** A ring R is a *semisimple ring* if every left R-module is semisimple.

Proposition 9.4. *The following facts are equivalent.*

1. *R is semisimple.*
2. *R is semisimple as a left R-module.*

3. Every short exact sequence of R-modules splits.

Proof. (3) $\Leftrightarrow$ (1). By definition.

(1) $\Rightarrow$ (2). Trivial.

(2) $\Rightarrow$ (1). Let M be an R-module. Then there exists a subset I such that $R^{(I)} \twoheadrightarrow M$. Since R is semisimple, by Theorem 9.2 $R^{(I)}$ is semisimple and by Proposition 9.1 M is also semisimple. □

Example. Let $R = D$ be a division ring. If $x \in D$, $x \neq 0$, then $Dx = D$. Hence, D has exactly two submodules, namely 0 and D, and it is simple as a left D-module. In particular, D is semisimple. Every simple D-module is isomorphic to $D/(\text{maximal left ideal}) = D$.

Every D-module is semisimple and it is the direct sum of copies of D.

Lemma 9.5. *It holds that $D^{(I)} \cong D^{(J)} \Leftrightarrow \#I = \#J$.*

Proof. ($\Leftarrow$). Trivial.

($\Rightarrow$). If I is finite, then the D-length of $D^{(I)}$ is equal to $\#I$. Hence, $D^{(J)}$ also has finite length and $\#J = l_D(D^{(J)}) = l_D(D^{(I)}) = \#I$.

If I is infinite, then J is also infinite. Let f be an isomorphism $D^{(I)} \xrightarrow{\sim} D^{(J)}$ and let $(e_i)_{i\in I}$ be the canonical basis of $D^{(I)}$.

Define $J_i := \{j : \text{the } j\text{-th coordinate of } f(e_i) \neq 0\} \subset J$. Since f is surjective, $J = \bigcup_{i\in I} J_i$.

Thus, $\#J \leq \sum_{i\in I} \#J_i \leq \#I \cdot \#Z = \#I$. By symmetry we get $\#J \leq \#I$, and therefore $\#I = \#J$. □

Theorem 9.6 (Maschke)**.** *Let k be a field and G be a finite group with* char $k \nmid \#G$ *(for instance, if* char $k = 0$*). Then $k[G]$ is semisimple.*

Proof. Suppose that we have a short exact sequence $0 \to L \to M \xrightarrow{p} N \to 0$ of $k[G]$-modules. If we consider this sequence as a sequence of k-modules, then it splits, because k is semisimple. Hence, there exists a k-linear map $q : N \to M$ such that $pq = \mathrm{id}_N$.

Define $r : N \to M$ by

$$r = \frac{1}{\#G} \sum_{\tau\in G} \tau q \tau^{-1} \qquad (\text{in } \mathrm{Hom}_k(N, M)).$$

Then we have

$$pr = \frac{1}{\#G} \sum_{\tau\in G} p\tau q\tau^{-1} = \frac{1}{\#G} \sum_{\tau\in G} \mathrm{id}_N = \mathrm{id}_N,$$

because p is a $k[G]$-linear map.

We also have that for $\sigma \in G$

$$\sigma r \sigma^{-1} = \frac{1}{\#G} \sum_{\tau\in G} p\sigma\tau q(\sigma\tau)^{-1} = r.$$

Thus, r is $k[G]$-linear and r gives a splitting of the sequence. □

Proposition 9.7. *Let $R \cong \bigoplus_{i\in I} S_i$ as a left R-module, with S_i simple for every $i \in I$. Then I is finite and every simple R-module is isomorphic to one of the S_i.*

Proof. Let $f : R \to \bigoplus_{i\in I} S_i$ be a left R-module isomorphism. Let $f(1) = (a_i)_{i\in I} \in \bigoplus_{i\in I} S_i$. Define $J := \{i \in I : a_i \neq 0\}$, a finite subset of I. Now we have $f(1) \in \bigoplus_{i\in J} S_i$ and therefore $Rf(1) \subset \bigoplus_{i\in J} S_i$. Since f is R-linear and surjective, we get $Rf(1) = f(R1) = f(R) = \bigoplus_{i\in I} S_i$. Thus, $\bigoplus_{i\in I} S_i \subset \bigoplus_{i\in J} S_i \subset \bigoplus_{i\in I} S_i$ and $I = J$, that is I is finite.

Now $R \cong_R S_1 \oplus S_2 \oplus \ldots \oplus S_n$ for an $n \in \mathbb{Z}$. The ring R has a composition series where only the S_i occur as quotients and therefore it has finite length.

Let S be a simple R-module, then $S \cong R/L$ for a maximal left ideal $L \subset R$. We have $0 \subset L \subset R$ and L has finite length, that is L has a composition chain. In this way we find a composition chain of R. This chain is Jordan-Hölder isomorphic to the composition chain where only the S_i occur. Hence, $S \cong S_i$ for an i. □

Corollary 9.8. *If R is semisimple and the S_i are as in Proposition 9.7, then every R-module is isomorphic to an R-module of the form $\bigoplus_{i\in I} S_i^{(V_i)}$ for certain sets V_i.*

Example. Let D be a division ring, $n \in \mathbb{Z}_{>0}$ and $R = M(n, D)$. Then the following facts true.

1. $S = D^n$ is a simple R-module. (We consider D^n as the set of column vectors of n elements of D.)
2. $R = S^n$ as a left R-module, R is semisimple, S is up to isomorphism the unique simple R-module and every R-module is isomorphic to $S^{(V)}$ for a set V.
3. The map $\varphi : D^{\mathrm{opp}} \xrightarrow{\sim} {}_R\mathrm{End}(S)$ given by $d \mapsto (x \mapsto xd)$ is a ring isomorphism.

Proof. 1. Consider D^n as a right D-module. Then $R = \mathrm{End}_D(D^n)$. If $x \in D^n$, $x \neq 0$, then $xD \cong_D D$, where $xd \leftrightarrow d$. Thus,

$$\begin{array}{rcl} D^n = (xD) \oplus (\text{complement}) & \xrightarrow{f} & D \\ (xd, \ldots) & \longmapsto & d \end{array}$$

is surjective. The composition of f with the inclusion $f_i : D \to D^n$, $d \mapsto de_i$, where e_i is the i-th vector of the canonical basis, gives for the element $x \in xD$ the following: $x = (x, 0) \overset{f}{\longmapsto} 1 \longmapsto e_i$. Since this composite map is a D-linear endomorphism of D^n, it is an element r_i of R. Thus, for every $i = 1, \ldots, n$ there is an $r_i \in R$ with $r_i x = e_i$. We have $e_1, \ldots, e_n \in Rx$ and therefore $D^n \subset Rx \subset D^n$, that is $Rx = D^n$. Hence, D^n is a simple R-module.

2. The proof that $R = S^n$ is the same as the one for fields. R is clearly semisimple. The rest of the argument follows from Proposition 9.7.

3. The map $f : D \to {}_R\mathrm{End}(S)$ given by $d \mapsto (x \mapsto xd)$ is well-defined, because $(Ax)d = A(xd)$ for all $A \in R$ and $d \in D$. Furthermore, we see that for all $d_1, d_2 \in D$ we have $d_1 + d_2 \mapsto (x \mapsto x(d_1 + d_2)) = (x \mapsto xd_1 + xd_2) = (x \mapsto xd_1) + (x \mapsto xd_2)$. Thus, for all $d_1, d_2 \in D$ we get $f(d_1 + d_2) = f(d_1) + f(d_2)$ and f is a group homomorphism.

   From the associativity of D it follows that for all $d_1, d_2 \in D$ we have $(x \mapsto x(d_1 d_2)) = (x \mapsto (xd_1)d_2)$ and therefore for all $d_1, d_2 \in D$ we get $f(d_1 d_2) = f(d_1) \circ f(d_2)$. It is clear that $f(1) = \mathrm{id}$.

   We see that f is a ring antihomomorphism. Thus, $f : D^{\mathrm{opp}} \to {}_R\mathrm{End}(S)$ is a ring homomorphism of D^{opp}.

   We still need to prove that f is bijective. Suppose that $\delta : S \to S$ is an R-linear endomorphism. We look for a $d \in D$ with $f(d) = \delta$, that is $\forall x \in S : \delta(x) = xd$. Since δ is R-linear,

for all $r \in R$ and $x \in S$ we have $\delta(rx) = r\delta(x)$. Thus, for every $r \in R$, δ maps the set rS into rS.

Apply this with r the matrix with 1 at position (i, i) and 0 elsewhere. We have

$$rS = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ D \\ 0 \\ \vdots \\ 0 \end{pmatrix} = e_i D.$$

Thus, $\delta(e_i) = e_i d_i$ voor een $d_i \in D$ and

$$\delta \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 d_1 \\ a_2 d_2 \\ \vdots \\ a_n d_n \end{pmatrix}.$$

Now take

$$r = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix}.$$

We get

$$rS = \left\{ \begin{pmatrix} a \\ a \\ \vdots \\ a \end{pmatrix} : a \in D \right\}.$$

Hence,

$$\delta \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ a \\ \vdots \\ a \end{pmatrix}$$

for an $a \in D$. On the other hand, we already know that

$$\delta \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}.$$

It follows that $a = d_1 = d_2 = d_3 = \ldots = d_n$. Thus, for all $x \in S$ we have $\delta(x) = xd$ for a $d \in D$. The map f is surjective.

It is easy to see that f is also injective, because the kernel of f is a two-sided ideal in the division ring D and it is therefore equal to 0.

□

Define $D' = ({}_R\operatorname{End}(S))^{\mathrm{opp}}$. Note that $D^{\mathrm{opp}} \cong (D')^{\mathrm{opp}}$. Now φ induces an isomorphism $R \to \operatorname{End}_{D'}(S) \cong M(n, D')$.

Corollary 9.9. *Let $n \in \mathbb{Z}_{>0}$ and let k be a field. Then $Z(M(n,k)) = k$.*

Proof. $\supset$: Clear.

$\subset$: If $r \in Z(M(n,k))$, Then the map $S = k^n \xrightarrow{r} k^n$; $x \mapsto rx$ is $M(n,k)$-linear. Indeed, if $rs = sr$ for $s \in M(n,k)$, then $r(sx) = s(rx)$. Hence, $r \in {}_R\operatorname{End}(S) = k$. □

Theorem 9.10. *Let $t \in \mathbb{Z}_{\geq 0}$, $D_1, D_2, \ldots, D_t$ division rings and $R = \prod_{i=1}^t M(n_i, D_i)$. Then the following facts are true.*

1. *The ring R is semisimple.*
2. *For every $i \in \{1, \ldots, t\}$ the module $S_i = D_i^{n_i}$ is a simple R-module.*
3. *$R \cong \bigoplus_{i=1}^t S_i^{n_i}$ as an R-module.*
4. *Every simple R-module is isomorphic to S_i for a unique $i \in \{1, 2, \ldots, t\}$.*
5. *$D_i^{\mathrm{opp}} \cong {}_R\operatorname{End}(S_i)$.*

Proof. We know that $R = R_1 \times R_2 \times \ldots \times R_t$, where $R_i = M(n_i, D_i)$. By the previous example we have that for all $i \in \{1, 2, \ldots, t\}$ the R_i-module $S_i = D_i^{n_i}$ is simple and that ${}_{R_i}R_{R_i} \cong S_i^{n_i}$. Thus, ${}_R R_R \cong \bigoplus_{i=1}^t S_i^{n_i}$. It also follows from the same example that every simple R-module is isomorphic to S_i for a unique $i \in \{1, 2, \ldots, t\}$ and that $D_i^{\mathrm{opp}} \cong {}_R\operatorname{End}(S_i)$. □

Theorem 9.11. *Let R be a semisimple ring. Then R is of the form $\prod_{i=1}^t M(n_i, D_i)$ with t, (n_i) and (D_i) as in Theorem 9.10. Furthermore, t, (n_i) and (D_i) are uniquely determined by R up to isomorphism.*

In the proof of this theorem we will use the following lemmas.

Lemma 9.12. *Let R be a ring. Then R and $({}_R\operatorname{End}(R))^{\mathrm{opp}}$ are isomorphic rings.*

Proof. The map $R \to ({}_R\operatorname{End}(R))^{\mathrm{opp}}$ given by $a \mapsto (x \mapsto xa)$ is a ring homomorphism with inverse $f \mapsto f(1)$. □

Lemma 9.13. *Let R be a ring, $M_1, M_2, \ldots, M_m$ and $N_1, N_2, \ldots, N_n$ be R-modules and let $M = \bigoplus_{i=1}^m M_i$ and $N = \bigoplus_{j=1}^n N_j$. Then ${}_R\operatorname{Hom}(M, N) \cong \bigoplus_{i,j} {}_R\operatorname{Hom}(M_i, N_j)$, where i runs over $1, \ldots, m$ and j over $1, \ldots, n$.*

Proof. Clear. □

Proof of Theorem 9.11. We know that ${}_R\operatorname{Hom}(S_i, S_j) = 0$ if $S_i \ncong S_j$. Moreover, ${}_R\operatorname{End}(S_i) = D_i$ is a division ring.

Suppose that $S_1, S_2, \ldots, S_t$ are all simple R-module and pairwise non-isomorphic. Choose $n_1, \ldots, n_t$ such that ${}_R R \cong \bigoplus_{i=1}^t S_i^{n_i}$. Then

$$\begin{aligned} {}_R\operatorname{End}(R) &= {}_R\operatorname{End}\Big(\bigoplus_{i=1}^t S_i^{n_i}\Big) = \prod_{i-1}^t {}_R\operatorname{End}(S_i^{n_i}) = \prod_{i=1}^t \prod_{\substack{1 \leq j \leq n_i \\ 1 \leq k \leq n_i}} {}_R\operatorname{Hom}(S_i, S_i) \\ &= \prod_{i=1}^t \prod_{j,k=1}^{n_i} D_i^{\mathrm{opp}} = \prod_{i=1}^t M(n_i, D_i^{\mathrm{opp}}). \end{aligned}$$

A simple calculation shows that if you choose well the identification $\prod_{j,k} D_i \xrightarrow{\sim} M(n_i, D_i^{\mathrm{opp}})$, then the resulting map ${}_R\operatorname{End}(R) \to \prod_{i-1}^{t} M(n_i, D_i^{\mathrm{opp}})$ is a ring isomorphism.

We have $R \cong ({}_R\operatorname{End}(R))^{\mathrm{opp}} \cong \prod_{i=1}^{t} M(n_i, D_i^{\mathrm{opp}})^{\mathrm{opp}} = \prod_{i=1}^{t} M(n_i, D_i)$. This last equality holds, because for $n \in \mathbb{Z}_{>0}$ and a division ring D we have that the map $M(n, D)^{\mathrm{opp}} \to M(n, D^{\mathrm{opp}})$ given by $A \mapsto A^T$ is an isomorphism. □

Note that $n_i = \operatorname{length}_{S_i} R$. For all $i \in \{1, \ldots, t\}$ the module S_i is a left D_i^{opp}-module and it is therefore a right D_i-module. Since $(rs)d = r(sd)$ for $r \in R$, $s \in S_i$ and $d \in D_i$, it is R-D_i-bimodule.

Theorem 9.14. *Let R be a simisimple ring, $k \subset Z(R)$ be a division ring which is a field, and let $[R : k] = \dim_k(R) < \infty$. Then $R \cong \prod_{i=1}^{t} M(n_i, D_i)$ met $t \in \mathbb{Z}_{>0}$, $n_i \in \mathbb{Z}_{>0}$ with $t \in \mathbb{Z}_{>0}$, $n_i \in \mathbb{Z}_{>0}$ and D_i a division ring with $k \subset Z(D_i)$ and $[D_i : k] < \infty$. Moreover, $\sum_{i=1}^{t} n_i^2 [D_i : k] = [R : k]$. If $k = \bar{k}$, then $D_i = k$ for all $i \in \{1, \ldots, t\}$ and $\sum_{i=1}^{t} n_i^2 = [R : k]$.*

Proof. Let $S_1, S_2, \ldots, S_t$ be as before. Then $\dim_k(S_i) < \infty$. By Theorem 9.11 it follows that $R \cong \prod_{i=1}^{t} M(n_i, D_i)$ with $n_i = \operatorname{length}_{S_i} R$ and $D_i = ({}_R\operatorname{End}(S_i))^{\mathrm{opp}} \subset (M(\dim_k(S_i), k))^{\mathrm{opp}}$. Hence, $k \subset Z(D_i)$.

The equality $\sum_{i=1}^{t} n_i^2 [D_i : k] = [R : k]$ is easily proved by comparing the dimensions in the equality $R \cong \prod_{i=1}^{t} M(n_i, D_i)$.

If $k = \bar{k}$, then by Theorem 8.11 we have $D_i = k$. □

Note that in the case $k = \bar{k}$ we have $S_i \cong D_i^{n_i} = k^{n_i}$ and thefore $n_i = \dim_k(S_i)$.

Example. Let $R = k[G]$ with G a group such that $\operatorname{char} k \nmid \#G < \infty$. Then $[R : k] = \#G$. If $k = \bar{k}$, then $\sum_{i=1}^{t} n_i^2 = \#G$.

Example. $k = \mathbb{C}$, $G = S_3$. Hence, $\#G = 6$.

We have a ring isomorphism $\mathbb{C}[S_3] \cong \prod_{i=1}^{t} M(n_i, \mathbb{C})$. By Theorem 9.14 it follows that $n_1^2 + n_2^2 + \ldots + n_t^2 = 6$. Now there are two options: either $t = 6$, $n_1 = n_2 = \ldots = n_6 = 1$, or $t = 3$, $n_1 = n_2 = 1$, $n_3 = 2$. Suppose the first case holds, then $M(1, \mathbb{C}) = \mathbb{C}$ and $\mathbb{C}[S_3] \cong \mathbb{C}^6$. Hence, $\mathbb{C}[S_3]$ is commutative and this is a contradiction. We are therefore in the second case: $t = 3$, $n_1 = n_2 = 1$ and $n_3 = 2$. We find that $\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times M(2, \mathbb{C})$. Up to isomorphism there are exactly three simple $\mathbb{C}[S_3]$-modules, two of $\mathbb{C}$-dimension 1 and one of $\mathbb{C}$-dimension 2. Which are these simple $\mathbb{C}[S_3]$-modules?

- $S_0 = \mathbb{C}$, with $\sigma x = x$ for all $x \in \mathbb{C}$, $\sigma \in S_3$
- $S_1 = \mathbb{C}$, with $\sigma x = \varepsilon(\sigma) x$ for all $x \in \mathbb{C}$, $\sigma \in S_3$ and $\varepsilon : S_3 \to \{\pm 1\}$ the sign homomorphism.
- We consider $\mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3$, $\sigma(e_i) = e_{\sigma(i)}$ for all $\sigma \in S_3$. Hence, $\sigma(e_1 + e_2 + e_3) = e_1 + e_2 + e_3$ for all $\sigma \in S_3$. Now we take $S_2 = \{(x_1, x_2, x_3) \in \mathbb{C}^3 : x_1 + x_2 + x_3 = 0\}$. Then $\dim_{\mathbb{C}}(S_0) = 2$. Since $\mathbb{C}[S_3]$ is semisimple, S_2 is in any case a direct sum of simple modules. Hence, either S_2 is simple, or S_2 is a direct sum of one-dimensional modules and we have the following options: $S_2 \cong S_0 \oplus S_0$, $S_0 \oplus S_1$ and $S_1 \oplus S_1$. On all these three modules A_3 acts as the identity map. Since A_3 do not act trivially on S_2, S_2 is simple.

If k is a field and G is a group, then the map

$$\begin{aligned} \operatorname{Hom}(G, k^*) &\longrightarrow \{k[G]\text{-modules of } k\text{-dimension } 1\}/\cong_{k[G]} \\ \chi &\longmapsto k_\chi = (k \text{ with } G\text{-action } \sigma(x) = \chi(\sigma)x, \text{ for } \sigma \in G \text{ and } x \in k) \end{aligned}$$

is a bijection, because the map $S \mapsto (\chi : G \to \operatorname{Aut}_k(S) \cong k^*)$ is the inverse. $\operatorname{Hom}(G, k^*)$ is a group. The corresponding group structure on the right side is given by $\otimes$. Hence, it holds that $k[G] \cong \prod_{i=1}^{t} M(n_i, k)$, with $\#\{i : n_i = 1\} = \#\operatorname{Hom}(G, k^*)$.

Example. Let $k = \bar{k}$, $\operatorname{char} k = 0$ and G be a finite abelian group. Then $k[G] \cong \prod_{i=1}^{t} M(n_i, k)$ and $\prod_{i=1}^{t} M(n_i, k)$ is therefore commutative, that is n_i are equal to 1. We know that $\sum_{i=1}^{t} n_i^2 = \#G$. Hence, $t = \#G = \#\mathrm{Hom}(G, k^*)$.

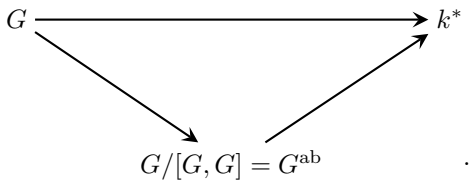
If $G = V_4 = \{1, \sigma, \tau, \sigma\tau\}$, then the matrix

1	σ	τ	$\sigma\tau$
1	1	1	1
1	-1	1	-1
1	1	-1	-1
1	-1	-1	1

gives the four homomorphisms $G \to k^*$. Hence, there are exactly four simple $k[V_4]$-modules, all of dimension 1.

Theorem 9.15. *Let $k = \bar{k}$,* $\operatorname{char} k = 0$ *and $\#G < \infty$. Then $\#\{i : n_i = 1\} = \#\mathrm{Hom}(G, k^*) = \#G/[G, G]$.*

Proof. We have the following diagram.



Any homomorphism $G \to k^*$ factors through $[G, G]$, because k^* is commutative and the image of all commutators is 1. Hence, $\mathrm{Hom}(G^{\mathrm{ab}}, k^*) \xrightarrow{\sim} \mathrm{Hom}(G, k^*)$. As in the example above it follows that $t = \#G/[G, G]$. □

Example. $\mathbb{C}[D_4]$, $D_4 = \langle \rho, \sigma \rangle$ with $\sigma\rho\sigma^{-1} = \rho^{-1}$ and $\sigma^2 = \rho^4 = 1$. Then $\#D_4 = 8$. Hence, $\sum_{i=1}^{t} n_i^2 = 8$, $\#\{i : n_i = 1\} = \#D_4/[D_4, D_4] = 4$, because $[D_4, D_4] = \langle \rho^2 \rangle$. We get $n_1 = n_2 = n_3 = n_4 = 1$, $n_5 = 2$ and $t = 5$. Since D_4 maps surjectively onto $D_4^{\mathrm{ab}} \cong V_4$, the 1-dimensional representations are the representations of V_4. Furthermore, k^2 with ρ and σ acting as

$$\rho = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

is a 2-dimensional representation. Note that ρ^2 acts nontrivially as -1 and therefore this representation is irreducible.

Theorem 9.16. *Let k an algebraically closed field and G be a finite group with* $\operatorname{char} k \nmid \#G$. *Then the number of isomorphism classes of simple $k[G]$-modules is equal to the number of conjugacy classes of G.*

Proof. $k[G] \cong \prod_{i=1}^{t} M(n_i, k)$. Hence, $Z(k[G]) \cong Z(\prod_{i=1}^{t} M(n_i, k)) = \prod_{i=1}^{t} Z(M(n_i, k)) =$

$\prod_{i=1}^{t} k$. Let $a \in Z(k[G])$, $a = \sum_{\sigma \in G} a_\sigma \sigma$ with $a_\sigma \in k$. Then

$$\begin{aligned} a \in Z(k[G]) &\Leftrightarrow \forall b \in k[G] : ab = ba \\ &\Leftrightarrow \forall \tau \in G : a = \tau a \tau^{-1} \\ &\Leftrightarrow \forall \tau \in G : \sum_{\sigma \in G} a_\sigma \sigma = \sum_{\rho \in G} a_{\tau^{-1}\rho\tau} \rho \\ &\Leftrightarrow \forall \sigma, \tau \in G : a_\sigma = a_{\tau^{-1}\sigma\tau} \\ &\Leftrightarrow a \text{ is of the form } \sum_{C \in G/\sim} a_C (\sum_{\sigma \in C} \sigma), \end{aligned}$$

where $G/\sim$ denotes the set of coniugacy classes of G. Therefore, $\{\sum_{\sigma \in C} \sigma : C \in G/\sim\}$ is a k-basis for $Z(k[G])$. If compare dimensions in the equality $Z(k[G]) \cong \prod_{i=1}^{t} k$, we find $\#(G/\sim) = t$. □

Example.

- $G = S_3$, $n_1 = n_2 = 1$, $n_3 = 2$, $t = 3$
- G abelian, $t = \#G$
- $G = D_4$, $t = 5$, the conjugacy classes are $\{1\}$, $\{\rho, \rho^{-1}\}$, $\{\sigma, \sigma\rho^2\}$, $\{\sigma\rho, \sigma\rho^3\}$ and $\{\rho^2\}$.

Chapter 10

Traces and characters

In this chapter k is an algebraically closed field of characteristic 0 and G is a finite group.

Definition 10.1 (Representation ring)**.** The Grothendieck group of the finite generated $k[G]$-modules is called *representation ring* $\mathcal{R}(G) = \mathcal{R}_k(G)$ of G.

Definition 10.2 (Character)**.** Let M be a finite generated $k[G]$-module with k-basis $\{e_1, \ldots, e_m\}$. Define for a $\sigma \in G$ the matrix $A_\sigma = (a_{ij})$ with a_{ij} given by $\sigma e_i = \sum_{j=1}^m a_{ij} e_j$. The *character* associated to M is the function

$$\begin{array}{rcl} \chi_M = \mathrm{Tr}_M : G & \longrightarrow & k \\ \sigma & \longmapsto & \mathrm{Tr}(A_\sigma). \end{array}$$

Moreover, $\chi_M(1)$ is the *dimension* of the character χ_M and $\chi_{M \oplus N} = \chi_M + \chi_N$.

Example. If $\chi : G \to k^*$ is a group homomorphism, we have a 1-dimensional $k[G]$-module via $k_\chi = k$ as a k-vector space and $\sigma x = \chi(\sigma)x$ for $\sigma \in G$, $x \in k_\chi$. It follows that $\chi_{k_\chi} = \chi$.

Note that group homomorphisms $G \to k^*$ are also called characters. Definition 10.2 is a general definition.

Definition 10.3 (Class function or central function)**.** A function $f : G \to k$ is a *class function* or a *central function* if $\forall \sigma, \tau \in G : f(\sigma\tau) = f(\tau\sigma)$, that is $\forall \sigma, \rho \in G : f(\sigma\rho\sigma^{-1}) = f(\rho)$, which is equivalent to require that f is constant on every conjugacy class of G

The vector space of class functions is denoted by $k^{G/\sim} \subset k^G$. Here $G/\sim$, also indicated by Γ, is the set of conjugacy classes of G.

Proposition 10.4. *Characters are class functions.*

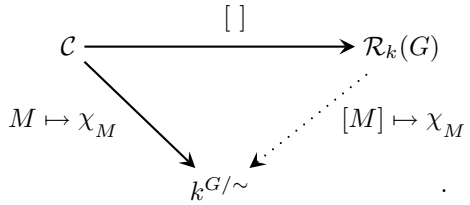
Proof. Let Tr_M be a character. Then for all $\sigma, \tau \in G$ we have $\mathrm{Tr}_M(\sigma\tau) = \mathrm{Tr}_M(\tau\sigma)$. It follows from linear algebra that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for matrices A and B. □

The map

$$\begin{array}{rcl} \mathcal{C} := \{\text{finitely generated } k[G]\text{-modules}\} & \longrightarrow & k^{G/\sim} \\ M & \longmapsto & \chi_M \end{array}$$

is additive. Indeed, if the sequence $0 \to M \to L \to N \to 0$ is exact, then it splits and L is isomorphic to $M \oplus N$. It also holds that $\chi_L = \chi_M + \chi_N$.

The universal property of the representation ring of G gives a unique group homomorphism $\mathcal{R}(G) \to k^{G/\sim}$ such that $[M]$ maps to χ_M.



Lemma 10.5. *It holds that* $\chi_{M\otimes_k N} = \chi_M\chi_N$*, where* $\chi_M\chi_N$ *is defined by* $(\chi_M\chi_N)(\sigma) = \chi_M(\sigma)\chi_N(\sigma)$ *for* $\sigma \in G$*.*

Proof. Exercise. □

If $M \cong \bigoplus_S S^{n_S}$, then $\chi_M = \sum_S n_S\chi_S$. Therefore, we may consider χ_S for all simple $k[G]$-modules S insted of χ_M for all $k[G]$-modules.

Definition 10.6 (Character table)**.** The *character table* of G is the matrix

$$\big[\chi_S(\sigma)\big]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim.}}$$

Here S runs over $\mathcal{S} = \{\text{simple } k[G]\text{-modules}\}/\cong$.

Example. We want to compute the character table of $G = S_3$ We already know that $G/\sim = \{1, (1\ 2), (1\ 2\ 3)\}$, $\mathcal{S} = \{1, \varepsilon, S_2\}$. The simple $k[G]$-modules 1 and ε are 1-dimensional k-vector spaces where G acts as the identity and as the sign homomorphism, respectively. S_2 is the 2-dimensional simple $k[G]$-module.

For all $\sigma \in G$ we have $\chi_1(\sigma) = 1$. For $S \in \mathcal{S}$ we also know that $\chi_S(1) = \dim_k(S)$. The other values in the character table are easily computed.

$S\backslash\sigma$	1	(1 2)	(1 2 3)
1	1	1	1
ε	1	-1	1
S_2	2	0	-1

Theorem 10.7. *The matrix* $\big[\chi_S(\sigma)\big]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim}}$ *is invertible.*

Proof. We have already seen that $k[G] \cong \prod_{S\in\mathcal{S}} \mathrm{End}_k(S)$. This means that there is an isomorphism $\varphi : Z(k[G]) \xrightarrow{\sim} \prod_{S\in\mathcal{S}} k$. It has also been proven that $\{\sum_{\sigma\in C}\sigma : C \in G/\sim\}$ is a k-basis for $Z(k[G])$. Let e_C be the C-th basis vector, that is $e_C := \sum_{\sigma\in C}\sigma$ for $C \in G/\sim$.

The S-th component of $\varphi(e_C)$ is $\alpha \in k$ if e_C acts on S as the multiplication by α. Then

$$\begin{aligned}
\alpha &= \frac{1}{\dim_k(S)}\mathrm{Tr}(\text{action of } e_C \text{ on } S)\\
&= \frac{1}{\dim_k(S)}\sum_{\sigma\in C}\chi_S(\sigma)\\
&= \frac{\#C}{\dim_k(S)}\chi_S(\sigma) \quad \text{for } \sigma \text{ in } C.
\end{aligned}$$

The map φ in the given basis is represented by the matrix

$$\left[\frac{\#[\sigma]}{\dim_k(S)}\chi_S(\sigma)\right]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim.}}$$

This matrix is invertible, because φ is an isomorphism. Since $\#[\sigma] \neq 0$, we get that $\big[\chi_S(\sigma)\big]_{\substack{S\in\mathcal{S}\\ \sigma\in G/\sim}}$ is invertible. □

Corollary 10.8. *The ring homomorphism*

$$\begin{aligned} \psi : \mathcal{R}(G) &\longrightarrow k^{G/\sim} \\ [M] &\longmapsto \chi_M \end{aligned}$$

is injective and induces a ring isomorphism $\psi' : \mathcal{R}(G) \otimes_{\mathbb{Z}} k \xrightarrow{\sim} k^{G/\sim}$.

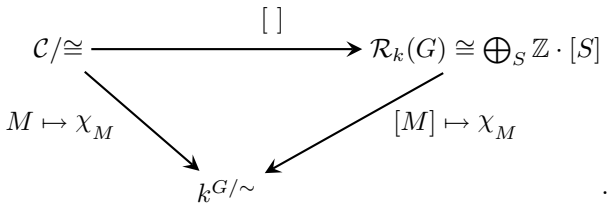
Proof. It is known that $\mathcal{R}(G) \cong \bigoplus_S \mathbb{Z} \cdot [S]$. Let $[M] = \sum_S n_S \cdot [S] \in \mathcal{R}(G)$. Then $\psi([M]) = \sum_S n_S \chi_S$. By Theorem 10.7 χ_S for $S \in \mathcal{S}$ are linearly independent over k. Hence, if $\sum_S n_S \chi_S = 0$, all n_S are equal to 0 (here we need that $\operatorname{char} k = 0$) and ψ is injective.

Since $\{[S] : S \in \mathcal{S}\}$ is a $\mathbb{Z}$-basis of $\mathcal{R}(G)$, $\{[S] \otimes 1 : S \in \mathcal{S}\}$ is a k-basis of $\mathcal{R}/G \otimes_{\mathbb{Z}} k$. The character table of G gives the matrix representation for ψ' and it is invertible. It follows that ψ' is an isomorphism. □

Corollary 10.9. *Every class function* $f : G \to k$ *is a unique* k*-linear combination of the* χ_S*, where* S *runs over* $\mathcal{S}$*.*

Definition 10.10 (Irreducible character)**.** If $S \in \mathcal{S}$, the character χ_S is an *irreducible character*. The set of irreducible characters of G is denoted by $X(G)$. Note that $X(G) \cong \mathcal{S}$.

Consider the following commutative diagram:



We map $k[G] \in \mathcal{C}$ in two ways to $k^{G/\sim}$.

Since $k[G] \cong_{k[G]} \prod_S \operatorname{End}_k(S)$, $k[G] \cong \bigoplus_S S^{\dim_k S}$ as a $k[G]$-module. Hence, $[k[G]] = \sum_S (\dim_k S)[S]$. It follows that $\chi_{k[G]} = \sum_{\chi \in X(G)} \chi(1)\chi$.

The matrix which represents the map $k[G] \to k[G]$ given by left multiplication by σ in the basis of all $\tau \in G$ is $[m_{\rho,\tau}]_{\rho,\tau}$, with $m_{\rho,\tau} = 1$ if $\rho = \sigma\tau$ and otherwise $m_{\rho,\tau} = 0$. The trace of this matrix is $\#G$ if $\sigma = 1$ and otherwise 0. This gives

$$\chi_{k[G]}(\sigma) = \begin{cases} \#G \text{ if } \sigma = 1 \\ 0 \text{ if } \sigma \neq 1. \end{cases}$$

The result is that for all $\sigma \in G$

$$\sum_{\chi \in X(G)} \chi(1)\chi(\sigma) = \begin{cases} \#G \text{ if } \sigma = 1 \\ 0 \text{ if } \sigma \neq 1. \end{cases}$$

Example. Let $G = D_4 = \langle \rho, \sigma : \sigma^2 = \rho^4 = 1, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle$. We have already seen that $D_4^{\mathrm{ab}} = D_4/\langle \rho^2 \rangle = V_4$. By a previous example we know that the simple $k[D_4]$-modules are four 1-dimensional modules (S_0, S_1, S_2, S_3) and one 2-dimensional module (S_4).

	1	σ	ρ	$\sigma\rho$	ρ^2
S_0	1	1	1	1	1
S_1	1	1	−1	−1	1
S_2	1	−1	1	−1	1
S_3	1	−1	−1	1	1
S_4	2	0	0	0	−2

Theorem 10.11. *Let M be a finitely generated $k[G]$-module and let $\sigma \in G$. Then $\chi_M(\sigma)$ is a sum of $\dim_k(M)$ roots of unity whose orders divide the order of σ.*

Proof. Firstly, consider the case with G abelian and M simple. Then $\dim_k(M) = 1$ and $M = k_\chi$ for a group homomorphism $\chi : G \to k^*$. Since G is finite, there is a natural number m such that $\sigma^m = 1$. We also have that $\chi_M(\sigma)^m = 1$ and therefore $\chi_M(\sigma)$ is a root of unity whose order divides m.

Now we consider the case G abelian and M not necessarily simple. Then $M = \bigoplus_{i=1}^t S_i$ with S_i simple and $t = \dim_k(M)$ and $\chi_M(\sigma) = \sum_{i=1}^t \chi_{S_i}(\sigma)$. We are again in the first case if we look at $\chi_{S_i}(\sigma)$.

The general case follows from the other cases. Indeed, consider M as a $k[\langle\sigma\rangle]$-module. The traces do not change. □

From now on $k = \mathbb{C}$ and G is a finite group.

Theorem 10.12. *Let M be a finitely generated $k[G]$-module and let $\sigma \in G$. Then $\chi_{M^\dagger}(\sigma) = \overline{\chi_M(\sigma)}$, where $\overline{\ }$ is the complex conjugation.*

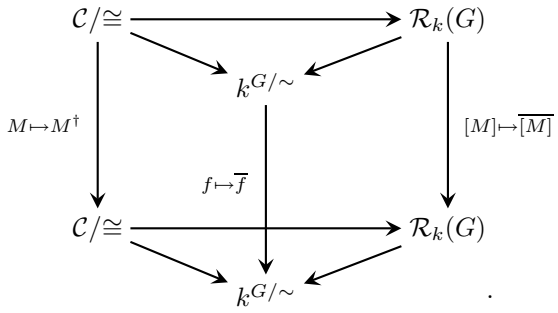
Proof. As in the proof of Theorem 10.11 we may reduce to the case where G is abelian and M is simple. Then again $M = k_\chi$ for a group homomorphism $\chi : G \to k^*$.

Let $f \in M^\dagger$. Then $(\sigma f)(x) = f(\chi(\sigma)^{-1}x) = \chi(\sigma)^{-1}f(x)$ for $x \in M$. Hence, $\sigma f = \chi(\sigma)^{-1}f$ and $(k_\chi)^\dagger = k_{\chi^{-1}}$. Since $\chi_M(\sigma)$ is a root of unity, we have $\chi_{M^\dagger}(\sigma) = \chi_M(\sigma)^{-1} = \overline{\chi_M(\sigma)}$. □

In conlusion, if we define

$$\begin{array}{rccl} \overline{\ } : k^{G/\sim} & \longrightarrow & k^{G/\sim} \\ f & \longmapsto & (\sigma \mapsto \overline{f(\sigma)}), \end{array}$$

then $\overline{\ }$ is a ring homomorphism of order 2 and the following diagram commutes.



Example. Let $G = C_3 \rtimes C_4$, where $C_3 = \langle\tau\rangle$, $C_4 = \langle\sigma\rangle$ and $\sigma\tau\sigma^{-1} = \tau^{-1}$. The conjugacy classes of G are $\{1\}$, $\{\tau, \tau^2\}$, $\{\sigma, \sigma\tau, \sigma\tau^2\}$, $\{\sigma^2\}$, $\{\sigma^2\tau\}$, $\{\sigma^3, \sigma^3\tau, \sigma^3\tau^2\}$.

Note that the number of elements in the conjugacy class of $x \in G$ is equal to $\#G/\#C_G(x)$. Here $C_G(x) := \{y \in G : xy = yx\}$ is the *centralizer* of x.

$G^{\mathrm{ab}} = \langle\sigma\rangle$. Thus, we need to write $\#G = 12$ as a sum of six squares, where four of them are equal to 1: $12 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2 + 2^2$. Hence, there are four 1-dimensional simple module and two 2-dimensional ones. Since $G/\langle\sigma^2\rangle \cong C_3 \rtimes C_2 \cong S_3$, the simple S_3-modules are also simple g-modules.

	1	τ	σ	σ^2	$\sigma^2\tau$	σ^3
	1	1	1	1	1	1
	1	1	i	-1	-1	$-i$
	1	1	-1	1	1	-1
	1	1	$-i$	-1	-1	i
	2	-1	0	2	-1	0
	2	-1	0	-2	1	0

Let M and N be $k[G]$-modules. Then $\mathrm{Hom}_{k[G]}(M,N)$ is a k-vector space. This induces a bilinear map

$$\begin{array}{rcl} \mathcal{R}(G)\times\mathcal{R}(G) & \longrightarrow & \mathbb{Z} \\ ([M],[N]) & \longmapsto & \dim_k \mathrm{Hom}_{k[G]}(M,N). \end{array}$$

The k-linear homomorphisms $\mathrm{Hom}_k(M,N)$ are a $k[G]$-module via the action $(\sigma f) : x \mapsto \sigma(f(\sigma^{-1}x))$ of $\sigma \in G$ on $f \in \mathrm{Hom}_k(M,N)$. This gives a map

$$\begin{array}{rcl} \mathcal{C}/{\cong}\times\mathcal{C}/{\cong} & \longrightarrow & \mathcal{C}/{\cong} \\ (M,N) & \longmapsto & \mathrm{Hom}_k(M,N). \end{array}$$

Lemma 10.13. *Let R be a commutative rinf and let M and N be R-modules. Assume that M is finitely generated and free, that is $M \cong_R R^n$. Then the map*

$$\begin{array}{rcl} \mathrm{Hom}_k(M,R)\otimes_R N & \longrightarrow & \mathrm{Hom}_R(M,N) \\ f\otimes y & \longmapsto & (x\mapsto f(x)y) \end{array}$$

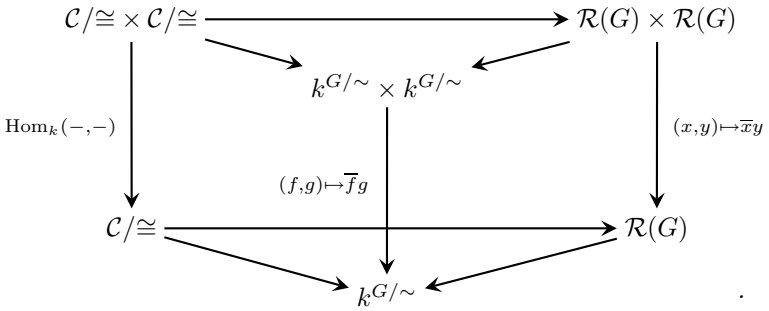
is an isomorphism of R-modules.

Proof. Exercise. □

Corollary 10.14. *If M and N are two finitely generated $k[G]$-modules, then $\mathrm{Hom}_k(M,N) \cong_{k[G]} M^\dagger \otimes_k N$.*

Proof. Lemma 10.13 gives a k-linear isomorphism. It also respects the G-action. □

Corollary 10.15. *The following diagram commutes.*



Lemma 10.16. *If we consider k as a $k[G]$-module where G acts trivially on k, then*

$$\begin{array}{rcl} \mathrm{Hom}_k(k,N) & \longrightarrow & N \\ f & \longmapsto & f(1) \end{array}$$

is a $k[G]$-linear isomorphism and

$$\begin{array}{rcl} \mathrm{Hom}_{k[G]}(k,N) & \longrightarrow & N^G = \{y \in N : \forall \sigma \in G : \sigma y = y\} \\ f & \longmapsto & f(1) \end{array}$$

is a k-linear isomorphism. Moreover, $\dim_k N^G = \frac{1}{\#G}\sum_{\sigma\in G}\chi_N(\sigma)$.

Proof. The given maps are well-defined isomorphism.

Define $\varphi = \sum_{\sigma\in G}(\#G)^{-1}\sigma \in k[G]$. Then for all $\tau \in G$ we have $\tau\varphi = \varphi$. Show that φ induces an exact sequence $0 \to \ker\varphi \to N \xrightarrow{\varphi} N^G \to 0$ of k-modules and that the inclusion $N^G \subset N$ gives a splitting of this sequence.

This means that $N \cong_k N^G \oplus \ker\varphi$. Since φ acts on N^G as the identity and on $\ker\varphi$ as 0, the trace of the action of φ on N is equal to $\dim_k N^G$. By definition of φ it follows that the trace of the action of φ on N is also equal to $\frac{1}{\#G}\sum_{\sigma\in G}\chi_N(\sigma)$. □

Theorem 10.17. *If M and N are finitely generated $k[G]$-modules, then*

$$\dim_k \mathrm{Hom}_{k[G]}(M,N) = \frac{1}{\#G}\sum_{\sigma\in G}\chi_M(\sigma)\overline{\chi_N(\sigma)}.$$

Proof. By Lemma 10.16 we have

$$(\mathrm{Hom}_k(M,N))^G = \{f \in \mathrm{Hom}_k(M,N) : \forall\sigma\in G : \sigma f = f\} = \mathrm{Hom}_{k[G]}(M,N).$$

It follows that

$$\dim_k \mathrm{Hom}_{k[G]}(M,N) = \frac{1}{\#G}\sum_{\sigma\in G}\chi_{\mathrm{Hom}_k(M,N)}(\sigma) = \frac{1}{\#G}\sum_{\sigma\in G}\overline{\chi_M(\sigma)}\chi_N(\sigma).$$

□

We define $\langle [M],[N]\rangle = \frac{1}{\#G}\sum_{\sigma\in G}\chi_M(\sigma)\overline{\chi_N(\sigma)}$. By Theorem 10.17 it follows that the bilinear map $\mathcal{R}(G)\times\mathcal{R}(G) \to \mathbb{Z}$ can be written as

$$\begin{array}{rcl} \mathcal{R}(G)\times\mathcal{R}(G) & \longrightarrow & \mathbb{Z} \\ ([M],[N]) & \longmapsto & \dim_k \mathrm{Hom}_{k[G]}(M,N) = \langle [M],[N]\rangle. \end{array}$$

If we define for $f, g \in k^{G/\sim}$, in an analogous way, $\langle f,g\rangle = \frac{1}{\#G}\sum_{\sigma\in G} f(\sigma)\overline{g(\sigma)}$, we get the following commutative diagram:

$$\begin{array}{ccc} \mathcal{R}(G)\times\mathcal{R}(G) & \xrightarrow{\langle -,-\rangle} & \mathbb{Z} \\ \downarrow & & \downarrow \\ k^{G/\sim}\times k^{G/\sim} & \xrightarrow[\langle -,-\rangle]{} & k. \end{array}$$

Note that if S and S' are simple modules, $\langle [S],[S']\rangle$ is equal to 1 if $[S] = [S']$ and to 0 otherwise. It is also true for irreducible characters χ and ψ that $\langle\chi,\psi\rangle$ is equal to 1 if $\chi = \psi$ and to 0 otherwise.

If $M = \sum_{S\in\mathcal{S}} n_S[S]$ with $n_S \in \mathbb{Z}$, $n_S \geq 0$, then $\langle [M],[M]\rangle = \sum_S n_S^2$. Hence, if M is a finitely generated $k[G]$-module, M is irreducible if and only if $\langle [M],[M]\rangle = 1$, that is if and only if $\langle\chi_M,\chi_M\rangle = 1$.

Lemma 10.18. *Let $f \in k^{G/\sim}$. There is a finitely generated $k[G]$-module M with $f = \chi_M$ if and only if $\forall \chi \in X(G) : \langle f, \chi \rangle \in \mathbb{Z}_{\geq 0}$.*

Proof. Write $f = \sum_{\chi \in X(G)} a_\chi \chi$, with $a_\chi \in k$. Then for all $\psi \in X(G)$ we have $\langle f, \psi \rangle = \sum_\chi a_\chi \langle \chi, \psi \rangle = a_\psi$.

Now suppose that $\forall \psi \in X(G) : \langle f, \psi \rangle \in \mathbb{Z}_{\geq 0}$ and define $M := \bigoplus_{S \in \mathcal{S}} S^{\langle f, \chi_S \rangle}$. Thus, $\chi_M = \sum_S \langle f, \chi_S \rangle \chi_S = f$.

Conversely, if $M = \bigoplus_S S^{n_S}$, then $\chi_M = \sum_S n_S \chi_S = \sum_S \langle f, \chi_S \rangle \chi_S$. □

Theorem 10.19. *For $\sigma, \tau \in G$*

$$\sum_{\chi \in X(G)} \chi(\sigma)\overline{\chi(\tau)} = \begin{cases} \frac{\#G}{\#[\sigma]} = \#C_G(\sigma) & \text{if } \sigma \sim \tau \\ 0 \quad \text{if } \sigma \not\sim \tau. \end{cases}$$

Proof. Define $A = [\chi(\sigma)]_{\substack{\chi \in X(G) \\ \sigma \in G/\sim}}$ and $B = [\chi(\sigma)\sqrt{\#[\sigma]}]_{\substack{\chi \in X(G) \\ \sigma \in G/\sim}}$.

Then

$$B\overline{B^T} = \left[\sum_{\sigma \in G/\sim} \#[\sigma] \chi(\sigma) \overline{\psi(\sigma)} \right]_{\chi, \psi \in X(G)} = \#G \cdot I,$$

because all elements outside the diagonal are zero and the element on the diagonal are $\#[\sigma]$.

Note that it follows that $|\det A|^2 = \prod_{\sigma \in G/\sim} \frac{\#G}{\#[\sigma]} = \prod_\sigma \#C_G(\sigma)$.

Now we know that $B^{-1} = \frac{1}{\#G}\overline{B^T}$, and therefore $B^T\overline{B} = \#G \cdot I$.

Thus,

$$\begin{aligned} \#G \cdot I = B^T\overline{B} &= \left[\sum_{\chi \in X(G)} \sqrt{\#[\sigma]\#[\tau]} \chi(\sigma)\overline{\chi(\tau)} \right]_{\sigma, \tau \in G/\sim} \\ &= \left[\sqrt{\#[\sigma]\#[\tau]} \sum_{\chi \in X(G)} \chi(\sigma)\overline{\chi(\tau)} \right]_{\sigma, \tau \in G/\sim.} \end{aligned}$$

The elements on the diagonal are $\#[\sigma]$ and the element outside the diagonal are 0. This proves the theorem. □

Chapter 11

Integrality and Burnside's theorem

Lemma 11.1. *Let A be a commutative ring, M be a finitely generated A-module and $\varepsilon \in \mathrm{End}_A(M)$. Then there is a monic polynomial $f \in A[X]$ such that $f(\varepsilon) = 0$, that is, if $f = \sum a_i X^i$, $\sum a_i \varepsilon^i(m) = 0$ for all $m \in M$.*

Proof. We may give M an $A[X]$-module structure via $(\sum b_i X^i) \cdot m = \sum b_i \varepsilon^i(m)$ for $\sum b_i X^i \in A[X]$ and $m \in M$.

Write $M = \sum_{i=1}^{n} Am_i$ for $m_1, \ldots, m_n \in M$.

Claim. For all $l \in \{0, 1, \ldots, n\}$ there exists a monic polynomial $f \in A[X]$ such that for all $m \in M$ there exist $g_1, \ldots, g_l \in A[X]$ with $\deg g_i < \deg f$ and $f \cdot m = \sum g_i m_i$.

Proof of the claim. If $l = n$, take $f = X$. Then $X \cdot m = \varepsilon(m) = \sum b_i m_i$. Thus, take $g_i = b_i$.

Suppose the claim is true for $l > 0$. We prove that is also true for voor $l - 1$.

There are f and h_i such that $f \cdot m_l = \sum_{i=1}^{l} h_i \cdot m_i$ with $h_i \in A[X]$ and $\deg h_i < \deg f$.

Hence, $(f - h_l) \cdot m_l = \sum_{i=1}^{l-1} h_i \cdot m_i$. Note that $f - h_l$ is a monic polynomial of the same degree of f.

Now let m an arbitrary element of M. We know that there are g_i such that $f \cdot m = \sum_{i=1}^{l} g_i \cdot m_i$. Then

$$\begin{aligned}(f - h_l)f \cdot m &= \left(\sum_{i=1}^{l-1}(f - h_l)g_i \cdot m_i\right) + g_l(f - h_l) \cdot m_l \\ &= \left(\sum_{i=1}^{l-1}(f - h_l)g_i \cdot m_i\right) + \left(\sum_{i=1}^{l-1} g_l h_i \cdot m_i\right) \\ &= \sum_{i=1}^{l-1}((f - h_l)g_i + g_l h_i) \cdot m_i.\end{aligned}$$

For $f' := (f - h_l)f$ and $g_i' := (f - h_l)g_i + g_l h_i$ the claim is true for $l - 1$.

It follows that the claim holds for $l = 0$ and this proves the lemma. □

Definition 11.2 (Faithful module)**.** An R-module M is a *faithful module* if for all $r \in R \setminus \{0\}$ there exists $m \in M$ such that $rm \neq 0$. In other words, it is faithful if the map $R \to \mathrm{End}_{\mathbb{Z}}(M)$ given by $r \mapsto (m \mapsto rm)$ is injective.

Theorem 11.3. *Let $A \subset B$ be commutative rings and let $\alpha \in B$. Then the following facts are equivalent.*

1. *There is a monic polynomial $f \in A[X]$ with $f(\alpha) = 0$.*
2. *The subring ring $A[\alpha] \subset B$ is finitely generated as an A-module.*
3. *There is a subring $C \subset B$ with $A \subset C$, $\alpha \in C$ and C is finitely generated as A-module.*
4. *There is a faithful $A[\alpha]$-module M such that it is finitely generated as an A-module.*

Definition. *An element α which satisfies all these properties is* integral *over A.*

Proof. (1) $\Rightarrow$ (2). Suppose that $f = X^n + \sum_{i=0}^{n-1} a_i X^i \in A[X]$ is such that $f(\alpha) = 0$. Define $C := \sum_{i=0}^{n-1} \alpha^i A$. Then $\alpha^n \in C \subset A[\alpha]$. Note that C is a finitely generated A-module.

Since $\alpha - \alpha^j \in C$ for $0 \leq j \leq n-1$, $\alpha C \subset C$. Thus, for all $j \geq 0$ we have $\alpha^j C \subset C$, that is $A[\alpha]C \subset C$ and $A[\alpha] = C$. In particular, $A[\alpha]$ is finitely generated as an A-module.

(2) $\Rightarrow$ (3): Take $C = A[\alpha]$.

(3) $\Rightarrow$ (4): Take $M = C$. $A[\alpha] \subset C$. Thus, C is an $A[\alpha]$-module. Let $r \in A[\alpha]$, $r \neq 0$. Then $1r \neq 0$, and therefore M is faithful.

(4) $\Rightarrow$ (1): Apply Lemma 11.1 with $\varepsilon : m \mapsto \alpha m$. Then there is a monic polynomial $f \in A[X]$ such that $(m \mapsto f(\alpha)m) = 0$. Since M is faithful, we get $f(\alpha) = 0$. □

Let $A \subset B$ be commutative rings.

Definition 11.4 (Integral)**.** B is *integral* over A if every element of B is integral over A.

Definition 11.5 (Integrally closed)**.** A is *integrally closed* in B if every element $\alpha \in B \setminus A$ is not integral over A.

Theorem 11.6. *Let A be a unique factorization domain. Then A is integrally closed.*

Proof. Suppose that $\alpha \in Q(A)$ is integral over A. Write $a = \frac{u}{v}$ with $u, v \in A$ such that u and v do not have common prime factors.

Choose $a_i \in A$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Then $a_{n-1}u^{n-1}v + a_{n-2}^{n-2}v^2 + \ldots + a_0 v^n = -u^n$. Thus, $v | u^n$. It follows that $v \in A^*$ and $\alpha \in A$. □

Lemma 11.7. *If $A \subset C$ are rings such that C is finitely generated as an A-module and M is a finitely generated C-module, then M is also finitely generated as an A-module.*

Proof. Since C is finitely generated as an A-module, there exist an $n \in \mathbb{Z}_{>0}$ and a surjective A-linear homomorphism $A^n \to C$. There are also an $m \in \mathbb{Z}_{>0}$ and a surjective C-linear homomorphism $C^m \to M$. Thus, there exists a surjective A-linear homomorphism $A^{nm} \to C^m \to M$. □

Theorem 11.8. *Let $A \subset B$ be commutative rings. Then the integral closure of A in B is a subring of B, contains A and is integrally closed in B.*

Proof. Define $D := \{\alpha \in B : \alpha \text{ is integral over } A\}$, the integral closure of A in B. It is clear that $A \subset D$.

We want to prove that if $\alpha, \beta \in D$, then also $\alpha\beta$, $\alpha - \beta \in D$. Let α and β arbitrary elements of D. Since α is integral over A, $A[\alpha]$ is a finitely generated A-module. Since β is integral over A, β is also integral over $A[\alpha]$. Thus, $A[\alpha][\beta] = A[\alpha, \beta]$ is a finitely generated $A[\alpha]$-module. Applying Lemma 11.7 with $C = A[\alpha]$, $M = A[\alpha, \beta]$, we find that $A[\alpha, \beta]$ is finitely generated as an A-module. It is clear that $\alpha\beta$ and $\alpha - \beta$ are contained in $A[\alpha, \beta]$. By Theorem 11.3 it follows that $\alpha\beta$ and $\alpha - \beta$ are integral over A and therefore they are in D.

We still need to prove that, if $\beta \in B$ is integral over D, then $\beta \in D$. Let $\beta \in B$ be any integral element over D. Then there exist a monic polynomial $g = X^t + \alpha_{t-1}X^{t-1} + \ldots + \alpha_1 X + \alpha_0 \in D[X]$ such that $g(\beta) = 0$. Now we have the following chain of rings: $A \subset A[\alpha_0] \subset A[\alpha_0, \alpha_1] \subset \ldots \subset A[\alpha_0, \alpha_1, \ldots, \alpha_{t-1}] =: D'$. Every ring different from A in this chain is finitely generated as a module over the previous one, because the new α_i is integral over A and therefore also over $A[\alpha_0, \ldots, \alpha_{i-1}]$. By Lemma 11.7 D' is finitely generated as an A-module. Since β is integral over D, it is integral over D' and $D'[\beta]$ is finitely generated as a D'-module. Applying again Theorem 11.3 with $C = D'[\beta]$, we get that β is integral over A. □

Notation. We denote the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ by $\overline{\mathbb{Z}}$. Suppose that $a, b \in \mathbb{C}$. We write $b|a$ ("b divides a") if $a \in \overline{\mathbb{Z}}b$.

Note that $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. If $c|b$ and $b|a$, then $c|a$. If $b|a_1$ and $b|a_2$, then $b|a_1 \pm a_2$.

Let G be a finite group.

Theorem 11.9. *If M is a finitely generated $\mathbb{C}[G]$-module, then $\chi_M(\sigma) \in \overline{\mathbb{Z}}$ for all $\sigma \in G$.*

Proof. Let $n = \dim_{\mathbb{C}} M$. Then $\chi_M(\sigma)$ is a sum of n roots of unity. Every root of unity is a zero of a polynomial of the form $X^m - 1$. Hence, every root of unity belongs to $\overline{\mathbb{Z}}$. It follows that $\chi_M(\sigma) \in \overline{\mathbb{Z}}$. □

Example. $i \in \overline{\mathbb{Z}}$, because i is a root of unity.

$\frac{i}{2} \notin \overline{\mathbb{Z}}$, because, if $\frac{i}{2}$ belonged to $\overline{\mathbb{Z}}$, then $(-i)\frac{i}{2} = \frac{1}{2}$ would also belong to $\overline{\mathbb{Z}}$. Since $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, this is not the case.

Example. If $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, then $\alpha \in \overline{\mathbb{Z}} \Leftrightarrow f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[X]$.

Proof. $\Leftarrow$: Clear. $\Rightarrow$: Exercise. □

Lemma 11.10. *Let $t \in \mathbb{Z}_{>0}$ and let $\eta_1, \ldots, \eta_t \in \mathbb{C}$ be roots of unity. Write $s = \eta_1 + \ldots + \eta_t$ and suppose that $s \neq 0$. Then the following facts are equivalent.*

1. *$t|s$.*
2. *All η_i are equal.*
3. *$|s| = t$.*
4. *$|s| \geq t$.*

Proof. (2) $\Rightarrow$ (1). Trivial: $\frac{s}{t} = \eta_1 \in \overline{\mathbb{Z}}$.

(4) $\Rightarrow$ (3) $\Rightarrow$ (2). If $a, b \in \mathbb{C}$, then $|a + b| \leq |a| + |b|$. The equality holds if and only if $\mathbb{R}_{>0} \cdot a = \mathbb{R}_{>0} \cdot b$, that is the vector from 0 to a has the same direction as the vector from 0 to b. Similarly, for $a_1, \ldots, a_t \in \mathbb{C}^*$ we have $|\sum_{i=1}^t a_i| \leq \sum_{i=1}^t |a_i|$ abd the equality holds if and only if all vectors from 0 to a_i have the same direction.

We apply this with $a_i = \eta_i$. For $i = 1, \ldots, t$ we know that η_i is a root of unity and therefore $|\eta_i| = 1$. It follows that $|s| = |\sum_{i=1}^t \eta_i| \leq \sum_{i=1}^t |\eta_i| = t$ and $|s| = t$ if and only if all vectors from 0 to η_i are equal, that is all η_i are equal.

Assertion (4) states that $|s| \geq t$. Hence, we find that $|s| = t$ (Assertion (3)) and therefore $\eta_1 = \ldots = \eta_t$ (Assertion (2)).

(1) $\Rightarrow$ (4): The following most obvious "proof" is wrong and therefore it is not a proof. If $t|s$ then $\frac{s}{t} \in \overline{\mathbb{Z}}$. *Thus*, $\left|\frac{s}{t}\right| \geq 1$ and $|s| \geq t$. The mistake is the "thus" written in italic, because it is not true that every element of $\overline{\mathbb{Z}}$ different from 0 has absolute value ≥ 1. Even sums of roots of unity can have absolute value ≥ 1, for instance $|\zeta_5 + \zeta_5^4| < 1$ where $\zeta_5 = e^{\frac{2\pi}{5}}$).

Define $K = \mathbb{Q}(\eta_1, \ldots, \eta_t)$. It is clear that $s = \sum_{i=1}^{t} \eta_i \in K$. K is Galois over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(K/\mathbb{Q})$. For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $\sigma(s) = \sum_{i=1}^{t} \sigma(\eta_i)$, where $\sigma(\eta_i)$ is again a root of unity for all i. Thus, $0 < |\sigma(s)| \leq t$.

Since $\frac{s}{t}$ is integral over $\mathbb{Z}$, $\sigma(\frac{s}{t}) = \frac{\sigma(s)}{t}$ is also integral over $\mathbb{Z}$. Then $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t} \in \overline{\mathbb{Z}}$. We also know that $\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t} \in \mathbb{Q}$, because for all $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ it holds that $\tau\left(\prod_\sigma \frac{\sigma(s)}{t}\right) = \prod_\sigma \frac{\sigma(s)}{t}$. Since $s \neq 0$, $\sigma(s) \neq 0$ and we find $0 \neq \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t} \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Hence, $\left|\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \frac{\sigma(s)}{t}\right| \geq 1$ and $\left|\frac{s}{t}\right| = \prod_{\sigma \neq 1} \left|\frac{t}{\sigma(s)}\right| \geq 1$. □

Theorem 11.11. *Let G be a finite group, M be a finitely generated $\mathbb{C}[G]$-module and let $\sigma \in G$. An element $\tau \in G$ acts* as a scalar *on M if $\exists c \in \mathbb{C} : \forall x \in M : \sigma(x) = cx$. The following equivalences are true.*

1. *σ acts trivially on $M \iff \chi_M(\sigma) = \dim_{\mathbb{C}} M$.*
2. *σ acts as a scalar on $M \iff |\chi_M(\sigma)| = \dim_{\mathbb{C}} M$. If $M \neq 0$, this is equivalent to $\dim_{\mathbb{C}} M | \chi_M(\sigma)$.*

Proof. We may assume that $G = \langle \sigma \rangle$, so, in particular, we may assume that G is abelian. Then M is a direct sum of 1-dimensional $\mathbb{C}[G]$-modules and σ acts as the matrix

$$\begin{pmatrix} \eta_1 & 0 & \ldots & 0 \\ 0 & \eta_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \eta_t \end{pmatrix},$$

where $\eta_1, \ldots, \eta_t$ are roots of unity and $t = \dim_{\mathbb{C}} M$.

1. $\Rightarrow$: Trivial.

$\Leftarrow$: From $\chi_M(\sigma) = \dim_{\mathbb{C}} M$ it follows that $\eta_1 + \ldots + \eta_t = t$. Lemma 11.10 gives $\eta_1 = \ldots = \eta_t = 1$. Hence, σ acts trivially as the identity matrix. Note that *(1)* holds even if $M = 0$.

2. Note that the first equivalence holds if $M = 0$. Suppose that $M \neq 0$.

$\Rightarrow$. If σ acts as c, then c is a root of unity. Thus,$\chi_M(\sigma) = ct$, dus $|\chi_M(c)| = |ct| = t$.

$\Leftarrow$: $|\eta_1 + \ldots + \eta_t| = t$. Lemma 11.10 says that all η_i are equal. Then σ acts as a multiple of the identity matrix.

The proof of the second equivalence is the same by using the first statement in Lemma 11.10. □

Define the set $N := \ker(G \to \mathrm{Aut}_{\mathbb{C}} M)$ of elements of G which act trivially on M and the set $H := \ker(G \to (\mathrm{Aut}_{\mathbb{C}} M)/\mathbb{C}^*)$ of elements of G which act on M as a scalar. The situation is the following: $N \subset H \subset G$ and both N and H are normal in G.

Definition 11.12. For a $\mathbb{C}[G]$-module M and $u \in \mathbb{C}[G]$, $\chi_M(u)$ is the trace of the action of u on M. Thus, $\chi_M : \mathbb{C}[G] \to \mathbb{C}$ is $\mathbb{C}$-linear.

Lemma 11.13. *Let $A \subset B_1$ and $A \subset B_2$ be commutative rings and embed A in $B_1 \times B_2$ via $a \mapsto (a, a)$. Then an element $(b_1, b_2) \in B_1 \times B_2$ is integral over A if and only if both b_1 and b_2 are integral over A.*

Proof. Exercise. □

Theorem 11.14. *Let G be a finite group and let $u \in Z(\mathbb{C}[G])$. Then*

$$\begin{aligned} u \in \overline{\mathbb{Z}}[G] &\implies u \text{ is integral over } \mathbb{Z} \\ &\iff \text{for all } \chi \in X(G) \text{ it holds that } \chi(1)|\chi(u). \end{aligned}$$

Proof. $\Rightarrow$. Define $B := \overline{\mathbb{Z}}[G] \cap Z(\mathbb{C}[G]) = \bigoplus_{C \in G/\sim} \overline{\mathbb{Z}} \sum_{\sigma \in G} \sigma$. B is finitely generated as a $\overline{\mathbb{Z}}$-module and therefore every element of B is integral over $\overline{\mathbb{Z}}$. Since $\overline{\mathbb{Z}}$ is integral over $\mathbb{Z}$, B is also integral over $\mathbb{Z}$.

$\Leftrightarrow$. The integral closure of $\mathbb{Z}$ in $Z(\mathbb{C}[G])$ is isomorphic to the integral closure of $\mathbb{Z}$ in $\prod_\chi \mathbb{C}$ under the isomorphism given by $u \mapsto \left(\frac{\chi(u)}{\chi(1)}\right)_{\chi \in X(G)}$. By Lemma 11.13 the integral closure of $\mathbb{Z}$ in $\prod_\chi \mathbb{C}$ is equal to $\prod_\chi \overline{\mathbb{Z}}$. Thus, u is integral over $\mathbb{Z} \Leftrightarrow \forall \chi \in X(G) : \frac{\chi(u)}{\chi(1)} \in \overline{\mathbb{Z}}$. □

Theorem 11.15. *For every $\chi \in X(G)$ it holds that $\chi(1)|\#G$.*

Proof. Take $u = \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma \in \mathbb{C}[G]$. We have $\chi(\sigma^{-1}) = \chi(\tau^{-1})$ if $\sigma \sim \tau$. Thus, $u \in Z(\mathbb{C}[G])$. Since all $\chi(\sigma^{-1}) \in \overline{\mathbb{Z}}$, we get $u \in \overline{\mathbb{Z}}[G]$. By Theorem 11.14 it follows that $\chi(1)|\chi(u)$. Moreover, we know that $\chi(u) = \sum_{\sigma \in G} \chi(\sigma)\overline{\chi(\sigma)}$. Since χ is an irreducible character, $\frac{1}{\#G} \sum_{\sigma \in G} \chi(\sigma)\overline{\chi(\sigma)} = 1$. Hence, $\sum_{\sigma \in G} \chi(\sigma)\overline{\chi(\sigma)} = \#G$ and $\chi(1)|\#G$. □

Theorem 11.16. *For every $\chi \in X(G)$ and every $\sigma \in G$ it holds that $\chi(1)|\#[\sigma]\chi(\sigma)$, where by $[\sigma]$ we mean the conjugacy class of σ.*

Proof. Take $u = \sum_{\substack{\tau \in G \\ \tau \sim \sigma}} \tau \in \mathbb{C}[G]$. We have $u \in Z(\mathbb{C}[G])$ and $u \in \overline{\mathbb{Z}}[G]$. By Theorem 11.14 it follows that $\chi(1)|\chi(u) = \#[\sigma]\chi(\sigma)$. □

Theorem 11.17. *Suppose that $\chi \in X(G)$ and $\sigma \in G$ satisfy $\gcd(\chi(1), \#[\sigma]) = 1$. Then either $\chi(\sigma) = 0$ or σ acts as a scalar on the simple $\mathbb{C}[G]$-module belonging to χ. In the latter case $\sigma\tau^{-1}$ acts as the identity on S for every $\tau \in G$ which is conjugated to σ.*

Proof. Write $\chi = \chi_S$. Then $\chi(1) = \dim_{\mathbb{C}} S = t$. We have $\chi(1)|\#[\sigma]\chi(\sigma)$ and $\chi(1)|\chi(1)\chi(\sigma)$. Since $\gcd(\chi(1), \#[\sigma]) = 1$, there exist integer numbers l and m such that $l\#[\sigma] + m\chi(1) = 1$. We know that $\chi(1)|l\#[\sigma]\chi(\sigma)$ and $\chi(1)|m\chi(1)\chi(\sigma)$. Thus, $\chi(1)|l\#[\sigma]\chi(\sigma) + m\chi(1)\chi(\sigma) = \chi(\sigma)$ and $t = \chi(1)|\chi(\sigma)$. By Lemma 11.10 it follows that either $\chi(\sigma) = 0$ or $\chi(\sigma) = t\eta$, for a root of unity η. In the second case σ acts as η. If τ is conjugated to σ, τ also acts as η. Hence, $\sigma\tau^{-1}$ acts as 1. □

Theorem 11.18 (Burnside)**.** *Let G be a finite group and let $\sigma \in G$ such that $\#[\sigma] = p^m$, with p prime and $m \in \mathbb{Z}_{>0}$. Then the subgroup $N = \langle \sigma\tau^{-1} : \tau \in [\sigma] \rangle$ is a normal subgroup of G with $\{1\} \subsetneq N \subsetneq G$.*

Proof. If $\rho \in G$, then

$$\rho\sigma\tau^{-1}\rho^{-1} = \rho\sigma\rho^{-1}\sigma^{-1}\sigma(\rho\tau\rho^{-1})^{-1} = (\sigma(\rho\sigma\rho^{-1})^{-1})^{-1}\sigma(\rho\tau\rho^{-1})^{-1} \in N.$$

Thus, N is a normal subgroup and $N \neq \{1\}$, because $\#[\sigma] > 1$. Since $\sigma \neq 1$, $\sum_{\chi \in X(G)} \chi(1)\chi(\sigma) = 0$. Then $\sum_{\substack{\chi \in X(G) \\ \chi \neq 1}} \chi(1)\chi(\sigma) = -1$. Hence, the prime p is not a divisor of $\sum_{\substack{\chi \in X(G) \\ \chi \neq 1}} \chi(1)\chi(\sigma)$. Choose $\chi \neq 1$ with $p \nmid \chi(1)\chi(\sigma)$. There exists a simple $\mathbb{C}[G]$-module S such that $\chi = \chi_S$. Since $\chi \neq 1$, χ acts nontrivially on S. We have that $p \nmid \chi(1)$ and therefore $\gcd(\chi(1), \#[\sigma]) = 1$. From $p \nmid \chi(1)\chi(\sigma)$ it follows that $\chi(\sigma) \neq 0$. Theorem 11.17 says that $\sigma\tau^{-1}$ acts as 1 on S for all $\tau \in [\sigma]$. Hence, N acts trivially on S and $N \neq G$. □

Theorem 11.19 ("Burnside's theorem" or "p^aq^b-Theorem")**.** *If G is a finite group and the number of prime numbers which divide $\#G$ is at most two, then G is solvable.*

Proof. We have already seen that this theorem is a corollary of Theorem 11.18. □

Chapter 12

The restriction map and Frobenius' theorem

Let G_1 and G_2 be groups. Let $\varphi : G_1 \to G_2$ be a group homomorphism. Then there is an induced ring homomorphism

$$\begin{array}{rcl} \mathbb{C}[G_1] & \longrightarrow & \mathbb{C}[G_2] \\ \sum\limits_{\sigma\in G_1}^{<\infty} a_\sigma \sigma & \longmapsto & \sum\limits_{\sigma\in G_1}^{<\infty} a_\sigma \varphi(\sigma) = \sum\limits_{\tau\in G_2} \left(\sum\limits_{\sigma\in\varphi^{-1}(\tau)} a_\sigma \right) \tau. \end{array}$$

Every $\mathbb{C}[G_2]$-module M becomes a $\mathbb{C}[G_1]$-module via the composite map $G_1 \xrightarrow{\varphi} G_2 \longrightarrow \mathrm{Aut}_{\mathbb{C}} M$, or, equivalently, $rx = \varphi(r)x$ for $r \in \mathbb{C}[G_1]$, $x \in M$ and φ the induced ring homomorphism. If confusion is possible, we denote the resulting $\mathbb{C}[G_1]$-module by $\varphi^* M$.

From now on we assume that the groups G_1 and G_2 are finite.

We have the following embeddings:

$$\{\text{f.g. } \mathbb{C}[G_2]\text{-modules}\}/\cong_{\mathbb{C}[G_2]} \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_2) \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_2) \otimes_{\mathbb{Z}} \mathbb{C} \cong \mathbb{C}^{G_2/\sim}$$

$$\{\text{f.g. } \mathbb{C}[G_1]\text{-modules}\}/\cong_{\mathbb{C}[G_1]} \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_1) \hookrightarrow \mathcal{R}_{\mathbb{C}}(G_1) \otimes_{\mathbb{Z}} \mathbb{C} \cong \mathbb{C}^{G_1/\sim}.$$

By using φ we are going to construct induced vertical maps.

The group homomorphism $\varphi : G_1 \to G_2$ induces a map

$$\begin{array}{rcl} \varphi^* : \{\text{f.g. } \mathbb{C}[G_2]\text{-modules}\}/\cong_{\mathbb{C}[G_2]} & \longrightarrow & \{\text{f.g. } \mathbb{C}[G_1]\text{-modules}\}/\cong_{\mathbb{C}[G_1]} \\ M & \longmapsto & \varphi^* M. \end{array}$$

If $0 \to L \to M \to N \to 0$ is a short exact sequence of finitely generated $k[G_2]$-modules, the sequence $0 \to \varphi^* L \to \varphi^* M \to \varphi^* N \to 0$ is a short exact sequence of finitely generated $k[G_1]$-modules. Thus, $M \mapsto [\varphi^* M] \in \mathcal{R}_{\mathbb{C}}(G_1)$ is additive and there is a unique *group* homomorphism $\varphi^* : \mathcal{R}_{\mathbb{C}}(G_2) \to \mathcal{R}_{\mathbb{C}}(G_1)$ such that $[M] \mapsto [\varphi^* M]$.

If $g \in \mathbb{C}^{G_2/\sim}$, then g is a map $G_2/\sim \to \mathbb{C}$. The homomorphism $\varphi : G_1 \to G_2$ induces a map $\varphi/\sim : G_1/\sim \to G_2/\sim$. Now we have a map

$$\begin{array}{rcl} (\varphi/\sim)^* : \mathbb{C}^{G_2/\sim} & \longrightarrow & \mathbb{C}^{G_1/\sim} \\ g & \longmapsto & g \circ (\varphi/\sim). \end{array}$$

We also have the following vertical maps.

$$\begin{array}{ccccccc}
\{\text{f.g. } \mathbb{C}[G_2]\text{-modules}\}/\cong_{\mathbb{C}[G_2]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G_2/\sim} \\
\downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*\otimes\mathrm{id}} & & \downarrow{\scriptstyle (\varphi/\sim)^*} \\
\{\text{f.g. } \mathbb{C}[G_1]\text{-modules}\}/\cong_{\mathbb{C}[G_1]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G_1/\sim}.
\end{array}$$

It is clear that the two squares on the left are commutative.

Lemma 12.1. *The left square*

$$\begin{array}{ccc}
\mathcal{R}_{\mathbb{C}}(G_2)\otimes_{\mathbb{Z}}\mathbb{C} & \xrightarrow[\psi_1]{\sim} & \mathbb{C}^{G_2/\sim} \\
\downarrow{\scriptstyle \varphi^*\otimes\mathrm{id}} & & \downarrow{\scriptstyle (\varphi/\sim)^*} \\
\mathcal{R}_{\mathbb{C}}(G_1)\otimes_{\mathbb{Z}}\mathbb{C} & \xrightarrow[\psi_2]{\sim} & \mathbb{C}^{G_1/\sim}
\end{array}$$

is commutative.

Proof. Since $\chi_{\varphi^*M}(\sigma) = \chi_M(\varphi(\sigma))$, we have $\chi_{\varphi^*M} = \chi_M \circ \varphi$. Thus, $\psi_1(\varphi^* \otimes \mathrm{id}_{\mathbb{C}})$ and $(\varphi/\sim)^* \circ \psi_2$ concide on all elements of the form $[M] \otimes 1$. These elements span the C-vector space $\mathcal{R}_{\mathbb{C}}(G_2)$. Since the maps are C-linear, $\psi_1(\varphi^* \otimes \mathrm{id}_{\mathbb{C}})$ and $(\varphi/\sim)^* \circ \psi_2$ conside on $\mathcal{R}_{\mathbb{C}}(G_2)$. □

Theorem 12.2. *The maps $\varphi^* : \mathcal{R}_{\mathbb{C}}(G_2) \to \mathcal{R}_{\mathbb{C}}(G_1)$, $\varphi^* \otimes \mathrm{id} : \mathcal{R}_{\mathbb{C}}(G_2) \otimes_{\mathbb{Z}} \mathbb{C} \to \mathcal{R}_{\mathbb{C}}(G_1) \otimes_{\mathbb{Z}} \mathbb{C}$ and $(\varphi/\sim)^* : \mathbb{C}^{G_2/\sim} \to \mathbb{C}^{G_1/\sim}$ are ring homomorphisms.*

Proof. We will prove the ring homomorphisms only for the first map and for the last one.

For the first map it is sufficient to show that, if M and N are finitely generated $\mathbb{C}[G_2]$-modules, we have $\varphi^*(M \otimes_{\mathbb{C}} N) \cong \varphi^*M \otimes_C \varphi^*N$ as $\mathbb{C}[G_1]$-modules. Firstly, $\varphi^*(M \otimes_{\mathbb{C}} N)$ is equal to $M \otimes_C N$ where G_1 acts by $\sigma(x \otimes y) = \varphi(\sigma)(x \otimes y) = (\varphi(\sigma)x) \otimes (\varphi(\sigma)y)$. Moreover, $\varphi^*M \otimes_C \varphi^*N$ is equal to $M \otimes_{\mathbb{C}} N$ where G_1 acts by $\sigma(x \otimes y) = \sigma(x) \otimes \sigma(y) = (\varphi(\sigma)x) \otimes (\varphi(\sigma)y)$.

In general, if X and Y are sets and $\lambda : X \to Y$ is a map, the map

$$\begin{array}{rcl}
\lambda^* : \mathbb{C}^Y & \longrightarrow & \mathbb{C}^X \\
f & \longmapsto & f \circ \lambda
\end{array}$$

is a ring homomorphism. Here $\mathbb{C}^Y$ is a ring via $(fg)(y) = f(y)g(y)$ for $f, g \in \mathbb{C}^Y$ and $y \in Y$. If we apply this with $X = G_1/\sim$, $Y = G_2/\sim$, and $\lambda = (\varphi/\sim)$, we get that $(\varphi/\sim)^*$ is a ring homomorphism. □

As we have seen before, we can define an involution $\overline{}$ on $\mathcal{R}_{\mathbb{C}}(G_i)$, $\mathcal{R}_{\mathbb{C}}(G_i) \otimes_{\mathbb{Z}} \mathbb{C}$, and $\mathbb{C}^{G_i/\sim}$.

$$\begin{array}{ccccccc}
\{\text{f.g. } \mathbb{C}[G]\text{-modules}\}/\cong_{\mathbb{C}[G]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G/\sim} \\
\downarrow{\scriptstyle M\mapsto M^\dagger} & & \downarrow{\scriptstyle [M]\mapsto\overline{[M]}} & & \downarrow{\scriptstyle (x\otimes c)\mapsto(x^\dagger\otimes\bar{c})} & & \downarrow{\scriptstyle f\mapsto\overline{}\circ f} \\
\{\text{f.g. } \mathbb{C}[G]\text{-modules}\}/\cong_{\mathbb{C}[G]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G/\sim}.
\end{array}$$

Theorem 12.3. *The three ring homomorphisms φ^*, $\varphi^* \otimes \mathrm{id}_C$ and $(\varphi/\sim)^*$ commute with the involution $\overline{}$.*

Proof. We prove this only for $(\varphi/\sim)^*$.

In general, if X and Y are sets and $\lambda : X \to Y$ is a map, the following diagram commutes.

$$\begin{array}{ccc} \mathbb{C}^Y & \xrightarrow{f\mapsto \bar{}\circ f} & \mathbb{C}^Y \\ {\scriptstyle\lambda^*}\downarrow & & \downarrow{\scriptstyle\lambda^*} \\ \mathbb{C}^X & \xrightarrow{f\mapsto \bar{}\circ f} & \mathbb{C}^X \end{array}$$

Indeed, $\bar{} \circ (f \circ \lambda) = (\bar{} \circ f) \circ \lambda$.

Apply this with $X = G_1/\!\sim$, $Y = G_2/\!\sim$, and $\lambda = (\varphi/\!\sim)$. □

Note that it follows that these three ring homomorphisms also respect the map $(M, N) \mapsto \mathrm{Hom}_{\mathbb{C}}(M, N)$. Indeed, $\mathrm{Hom}_{\mathbb{C}}(M, N) \cong M^\dagger \otimes_C N$.

We have also previously constructed the following commutative diagram.

$$\begin{array}{ccccccc} (\{\text{f.g. } \mathbb{C}[G]\text{-modules}\}/\!\cong_{\mathbb{C}[G]})^2 & \hookrightarrow & (\mathcal{R}_{\mathbb{C}}(G))^2 & \hookrightarrow & (\mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C})^2 & \cong & (\mathbb{C}^{G/\sim})^2 \\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\psi'} & & \downarrow & & \downarrow{\scriptstyle\langle -,-\rangle} \\ \mathbb{Z}_{\geq 0} & \subset & \mathbb{Z} & \subset & \mathbb{C} & = & \mathbb{C} \end{array}$$

These are the vertical maps, from left to right:

$$\begin{aligned} \psi : (M, N) &\mapsto \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(M, N) \\ \psi' : ([M], [N]) &\mapsto \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(M, N) \\ (x \otimes c, y \otimes d) &\mapsto \psi'(x, y) c\bar{d} \\ (f, g) &\mapsto \langle f, g\rangle \end{aligned}$$

Theorem 12.4. *If φ is* surjective*, then φ^*, $\varphi^* \otimes \mathrm{id}_{\mathbb{C}}$, and $(\varphi/\!\sim)^*$ respect the inner product of the previous diagram. This means, for instance, that*

$$\begin{aligned} &\forall x, y \in \mathcal{R}_{\mathbb{C}}(G_2) : \psi'(x, y) = \psi'(\varphi^* x, \varphi^* y) \\ &\forall f, g \in \mathbb{C}^{G_2/\sim} : \langle f, g\rangle = \langle (\varphi/\!\sim)^*(f), (\varphi/\!\sim)^*(g)\rangle. \end{aligned}$$

Proof. We only have to prove that for finitely generated $\mathbb{C}[G_2]$-modules M and N we have $\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G_2]}(M, N) = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G_1]}(\varphi^* M, \varphi^* N)$.

In general, $\mathrm{Hom}_{\mathbb{C}[G_2]}(M, N) \subset \mathrm{Hom}_{\mathbb{C}[G_1]}(\varphi^* M, \varphi^* N)$. Since φ is surjective, the map $\mathbb{C}[G_1] \mapsto \mathbb{C}[G_2]$ induced by φ is also surjective. It follows that every $\mathbb{C}[G_1]$-linear map is also $\mathbb{C}[G_2]$-linear. Thus, $\mathrm{Hom}_{\mathbb{C}[G_2]}(M, N) = \mathrm{Hom}_{\mathbb{C}[G_1]}(\varphi^* M, \varphi^* N)$. In particular, the dimensions are equal. □

Let G be a finite group and H be a subgroup of G. We denote the inclusion map $H \to G$ by i. The usual notation for i^* is Res or Res^G_H and we call i^* the *restriction map*. Applying what we have seen above, we get the following commutative diagram.

$$\begin{array}{ccccccc} \{\text{f.g. } \mathbb{C}[H]\text{-modules}\}/\!\cong_{\mathbb{C}[H]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(H) & \subset & \mathcal{R}_{\mathbb{C}}(H) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{H/\sim} \\ \uparrow{\scriptstyle i^*} & & \uparrow{\scriptstyle i^*} & & \uparrow{\scriptstyle i^* \otimes \mathrm{id}} & & \uparrow{\scriptstyle (i/\sim)^*} \\ \{\text{f.g. } \mathbb{C}[G]\text{-modules}\}/\!\cong_{\mathbb{C}[G]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G) & \subset & \mathcal{R}_{\mathbb{C}}(G) \otimes_{\mathbb{Z}} \mathbb{C} & \cong & \mathbb{C}^{G/\sim}. \end{array}$$

Now we are going to prove Frobenius' theorem by using the above diagram.

Theorem 12.5 (Frobenius' theorem)**.** *Let G be a group which acts transitively on a finite set X and let $n_\sigma = \#\{x \in X : \sigma x = x\}$ for $\sigma \in G$. If $n_\sigma \leq 1$ for all $\sigma \in G$ and $\sigma \neq 1$, then $N = \{1\} \cup \{\sigma \in G : n_\sigma = 0\}$ is a normal subgroup of G with $\#N = \#X$.*

Example. Let $\mathbb{F}_q$ be a finite field and H be a subgroup of $\mathbb{F}_q^*$. Take $X = \mathbb{F}_q$ and $G = \{\sigma : X \to X : \exists a \in H, b \in \mathbb{F}_q : \forall x \in \mathbb{F}_q : \sigma x = ax + b\}$.

We have $\sigma 0 = b$ and $\sigma 1 = a$. Thus, $\#G = q \cdot \#H$ and then $\#G | (q-1)q$.

In order to compute n_σ, we have to determine the number of solutions of the equation $\sigma x = ax + b = x$ with $a \in H$ and $b \in \mathbb{F}_q$. This equality is equivalent to $(a-1)x = x$. Hence,

$$n_\sigma = \begin{cases} 1 & \text{als } a \neq 1 \\ 0 & \text{als } a = 1,\ b = 0 \\ q & \text{als } \sigma = 1 \end{cases} .$$

If $\#X = 1$, the theorem is easily seen to be true. From now on, suppose that $\#X = n > 1$. Let $\sigma \in \ker\varphi$, where φ is the map $G \to \mathrm{Sym}X = S_n$ given by $\tau \mapsto (x \mapsto \tau x)$. We have $n_\sigma = \#X > 1$ and $\sigma = 1$. Hence, φ is injective and G is isomorphic to a subgroup of S_n. Thus, G is finite.

Now fix $y \in X$ and let $H = \{\sigma \in G : \sigma y = y\}$ be the stabilizer of y. The map $\tau H \mapsto \tau y$ is an isomorphism $G/H \xrightarrow{\sim} X$. If $\tau, \rho \in G$ and $\tau H \neq \rho H$, then $\tau y \neq \rho y$. Thus, $\tau H \tau^{-1} \cap \rho H \rho^{-1} = \{\sigma \in G : \sigma\tau y = \tau y\} \cap \{\sigma \in G : \sigma\rho y = \rho y\} = \{1\}$. This is equivalent to the following statement: If $\tau \in G$, $\tau \notin H$, then $\tau H \tau^{-1} \cap H = \{1\}$. It is clear that the last statement follows from the previous one if we take $\rho = 1$. Conversely, the former one follows from the latter one by noticing that $\tau H \neq \rho H \Leftrightarrow \rho^{-1}\tau H \neq H$. From the second assertion we get $(\rho^{-1}\tau)H(\tau^{-1}\rho) \cap H = \{1\}$. Therefore, $\tau H \tau^{-1} \cap \rho H \rho^{-1} = \{1\}$.

Hence, $G \setminus \{1\} = (N \setminus \{1\}) \sqcup \coprod_{\tau H \in G/H}((\tau H \tau^{-1}) \setminus \{1\})$. Let $h = \#H$. Then $\#G = \#(G/H) \cdot \#H = nh$ and it follows that $nh - 1 = \#N - 1 + n(h-1)$. Thus, $nh = \#N + n(h-1)$ and $\#N = n = \#X$.

After these remarks we can reformulate Frobenius' theorem.

Theorem 12.6 (Reformulation of Frobenius' theorem)**.** *Let G be a finite group and H be a subgroup of G of index $n > 1$. Suppose that $\tau H \tau^{-1} \cap H = \{1\}$ for all $\tau \in G$ with $\tau \notin H$. Define $N = (G \setminus \bigcup_{\tau H \in G/H}(\tau H \tau^{-1})) \cup \{1\}$. Then N is a normal subgroup of G with $\#N = n$.*

Motivation of the proof.
Suppose that N is normal. Then $\#G/N = h$ and the composite map $H \to G/N$ of the inclusion map $H \to G$ and the projection map $G \to G/N$ is injective, because $H \cap N = \{1\}$. Hence, $H \cong G/N$ and there is a group homomorphism $\varphi : G \to H$ with $\varphi|_H = \mathrm{id}_H$, that is $\varphi i = \mathrm{id}_H$. The idea of the proof is the following one: Construct vertical maps in the above diagram which are one-sided inverses of the given vertical maps, going from right to left.

Proof. Let $\sigma \in H$, $\sigma \neq 1$. Then $\#[\sigma]_H = \frac{\#H}{\#C_H(\sigma)}$ and $\#[\sigma]_G = \frac{\#G}{\#C_G(\sigma)}$. Let $C_H(\sigma) = \{\tau \in H : \sigma\tau = \tau\sigma\}$ be the centralizer of σ in H. We define the centralizer $C_G(\sigma)$ in a similar way.

Let $\rho \in C_G(\sigma)$. Then $\rho\sigma\rho^{-1} = \sigma \in H \cap \rho H \rho^{-1}$, $H \cap \rho H \rho^{-1} \neq \{1\}$, and $\rho \in H$. Thus, $C_G(\sigma) = C_H(\sigma)$. It follows that $\#[\sigma]_G = \#[\sigma]_H \cdot n$. We see that $[\sigma]_G = \coprod_{\tau H \in G/H} \tau[\sigma]_H\tau^{-1}$ and $[\sigma]_G \cap H = [\sigma]_H$. The map i induces a bijection $(H \setminus \{1\})/\!\sim \to (G \setminus N)/\!\sim$.

Now define the map $\psi : G/\!\sim \to H/\!\sim$ by

$$\psi([\sigma]_G) = \begin{cases} [\sigma]_H = [\sigma]_G \cap H & \text{if } \sigma \in H \setminus \{1\} \\ [1]_H & \text{for } \sigma \in N \end{cases} .$$

Note that $\psi \circ (i/\!\sim) = \mathrm{id}_{H/\sim}$.

Define $\psi^* : \mathbb{C}^{H/\sim} \to \mathbb{C}^{G/\sim}$ by $\psi^*(f) = f \circ \psi$. It is clear that ψ^* is a ring homomorphism with $i^*\psi^* = \mathrm{id}_{\mathbb{C}^{H/\sim}}$.

Now define the map $\mathcal{R}_\mathbb{C}(H) \otimes_\mathbb{Z} \mathbb{C} \to \mathcal{R}_\mathbb{C}(G) \otimes_\mathbb{Z} \mathbb{C}$ by considering the isomorphism $\mathcal{R}_\mathbb{C}(G) \otimes_\mathbb{Z} \mathbb{C} \xrightarrow{\sim} \mathbb{C}^{G/\sim}$, the map $\psi : G/\!\sim \to H/\!\sim$ and the isomorphism $\mathbb{C}^{H/\sim} \xrightarrow{\sim} \mathcal{R}_\mathbb{C}(H) \otimes_\mathbb{Z} \mathbb{C}$.

We want to prove some properties of the map ψ^*.

Property 1. $\psi^* : \mathbb{C}^{H/\sim} \to \mathbb{C}^{G/\sim}$ preserves inner products, that is fot all $f, g \in \mathbb{C}^{H/\sim}$ it holds that $\langle f, g\rangle_H = \langle \psi^* f, \psi^* g\rangle_G$.

Proof.

$$\begin{aligned}\langle \psi^* f, \psi^* g\rangle_G &= \frac{1}{\#G}\sum_{\sigma\in G}\psi^* f(\sigma)\overline{\psi^* g(\sigma)} = \frac{1}{\#G}\sum_{[\sigma]_G\in G/\sim}\#[\sigma]_G f(\psi([\sigma]_G))\overline{g(\psi([\sigma]_G))}\\ &= \frac{1}{\#G}\sum_{C\in H/\sim}\left(\sum_{\substack{[\sigma]_G\in G/\sim\\ \psi([\sigma]_G)=C}}\#[\sigma]_G\right) f(C)\overline{g(C)}.\end{aligned}$$

We have

$$\sum_{\substack{[\sigma]_G\in G/\sim\\ \psi([\sigma]_G)=C}}\#[\sigma]_G = \begin{cases} n\cdot\#C & \text{if } C\neq\{1\}\\ \sum_{[\tau]_G\in G/\sim}\#[\tau]_G = \#N = n = n\cdot\#C & \text{if } C=1\end{cases}.$$

Thus, we get

$$\langle \psi^* f, \psi^* g\rangle_G = \frac{n}{\#G}\sum_{C\in H/\sim}\#C f(C)\overline{g(C)} = \frac{1}{\#H}\sum_{\sigma\in H} f(\sigma)\overline{g(\sigma)} = \langle f, g\rangle_H.$$

□

Property 2. For all $f\in\mathbb{C}^{H/\sim}$ and $g\in\mathbb{C}^{G/\sim}$ with $f(1)=0$ it holds that $\langle\psi^* f, g\rangle_G = \langle f, i^* g\rangle_H$. (Note that $i^* g = h|_H$.)

Proof.

$$\begin{aligned}\langle \psi^* f, g\rangle_G &= \frac{1}{\#G}\sum_{[\sigma]\in G/\sim} f(\psi(\sigma))\overline{g(\sigma)}\#[\sigma]_G = \frac{1}{\#G}\sum_{C\in H/\sim} f(C)\sum_{\substack{[\sigma]_G\in G/\sim\\ \psi([\sigma]_G)=C}}\#[\sigma]_G\overline{g(\sigma)}\\ &= \frac{1}{\#G}\sum_{\substack{C\in H/\sim\\ C\neq\{1\}}} f(C)n\#C\overline{g(C)} = \frac{1}{\#G}\sum_{C\in H/\sim} f(C)n\#C\overline{g(C)}\\ &= \frac{1}{\#H}\sum_{C\in H/\sim}\#C f(C)\overline{g(C)} = \langle f, g|_H\rangle_H.\end{aligned}$$

□

Property 3. It holds that $\psi^*(\mathcal{R}(H))\subset\mathcal{R}(G)$.

Proof. We have $\mathcal{R}(G) = \bigoplus_{S\text{ simpel}}\mathbb{Z}\cdot[S]\subset\mathcal{R}(G)\otimes\mathbb{C} = \bigoplus_S\mathbb{C}\cdot[S]\cong\bigoplus_{\chi\in X(G)}\mathbb{C}\cdot\chi$. We have already seen that

$$\langle[S],[S']\rangle = \begin{cases}1 & \text{if } [S]=[S']\\ 0 & \text{otherwise}\end{cases}.$$

If $\chi\in\mathcal{R}(G)\otimes\mathbb{C}$, then

$$x\in\mathcal{R}(G)\Leftrightarrow\forall\chi\in X(G):\langle x,\chi\rangle_G\in\mathbb{Z}, \tag{12.1}$$

as we already know.

We have to prove that $\psi^*(x)\in\mathcal{R}(G)$ for all $x\in\mathcal{R}(H)$ with $x(1)=0$. Let x any element of $\mathcal{R}(H)$ with $x(1)=0$ and let χ be any element of $X(G)$. It is sufficient to show that $\langle\psi^*(x),\chi\rangle_G\in\mathbb{Z}$.

From Property 2 we get $\langle \psi^*(x), \chi\rangle_G = \langle x, i^*\chi\rangle_H$. Since χ is simple, $\chi \in \mathcal{R}(G)$. Thus, $i^*\chi \in \mathcal{R}(H)$ and $i^*\chi = \sum_{\omega\in X(H)} n_\omega\omega$ with $n_\omega \in \mathbb{Z}$. We have $\langle x, i^*\chi\rangle_H = \sum_{\omega\in X(H)} n_\omega\langle x, \omega\rangle_H \in \mathbb{Z}$, because $\langle x, \omega\rangle \in \mathbb{Z}$ by (12.1). We have shown that $\langle \psi^*(x), \chi\rangle_G \in \mathbb{Z}$ for all $x \in \mathcal{R}(H)$ with $x(1) = 0$.

The map $\rho : \mathcal{R}(H) \to \mathbb{Z}$ given by $x \mapsto x(1)$ is a ring homomorphism. We have proved Property 2 only for elements in the kernel of ρ and we have seen that $\psi^*(\ker\rho) \subset \mathcal{R}(G)$. The function ρ maps 1 to 1. Thus, $\mathcal{R}(H) = (\ker\rho) \oplus \mathbb{Z}\cdot 1$. Since ψ^* also maps 1 to 1, we find that $\psi^*(\mathcal{R}(H)) \subset \mathcal{R}(G)$ and we are done. □

Property 4. For every $\chi \in X(H)$ it holds that $\psi^*\chi \in X(G)$ and N acts trivially on the simple $\mathbb{C}[G]$-module belonging to $\psi^*\chi$.

Proof. Let $\chi \in X(G)$. Then $\chi \in \mathcal{R}(H)$ and from Property 3 we have $\psi^*\chi \in \mathcal{R}(G)$. Let $\psi^*\chi = \sum_{\omega\in X(G)} n_\omega\omega$, with $n_{\omega\in\mathbb{Z}}$. We have to prove that one of the n_ω is equal to 1 and all the others are equal to 0. We know that $\langle \psi^*\chi, \psi^*\chi\rangle_G = \sum_{\omega\in X(G)} n_\omega^2$. It also follows from Property 1 that $\langle \psi^*\chi, \psi^*\chi\rangle_G = \langle \chi, \chi\rangle_H = 1$. Hence, all n_ω but one are equal to 0 and the last n_ω is equal to either 1 or -1.

Now $\chi\psi = \psi^*\chi = \pm\omega$ for an element $\omega \in X(G)$. Thus, $\chi\psi(1) = \pm\omega(1) \in \pm(\mathbb{Z}_{>0})$ and, on the other hand, $\chi\psi(1) = \chi(1) \in \mathbb{Z}_{>0}$. Hence, the last n_ω is equal to 1.

Let M be the $\mathbb{C}[G]$-module belonging to $\psi^*\chi$ and let $\tau \in N$. Then the trace of τ on M is equal to $\psi^*\chi(\tau) = \chi(\psi(\tau)) = \chi(1) = \chi(\psi(1))$, which is equal to the trace of 1 on M, that is equal to $\dim_{\mathbb{C}} M$. Hence, τ acts on M as 1. □

Remark. We can $\mathcal{R}(G)$ write as $\mathcal{R}(G) = \sum_{\chi\in X(G)} \mathbb{Z}\cdot\chi$. Now we get $\mathcal{R}(G)_{\text{eff}} = \sum_{\chi\in X(G)} \mathbb{Z}_{\geq 0}\cdot\chi$. From Property 4 it follows that $\psi^*(\mathcal{R}(H)_{\text{eff}}) \subset \mathcal{R}(G)_{\text{eff}}$.

By this remark there is a map

$$\begin{array}{rcl} \psi^* : \{\text{f.g. } \mathbb{C}[H]\text{-modules}\}/\cong & \longrightarrow & \{\text{f.g. } \mathbb{C}[G]\text{-modules}\}/\cong \\ M & \longmapsto & \psi^*M \end{array}$$

with the following properties.

- N acts trivially on every ψ^*M. (If M is simple, we know that by Property 4. For non-simple M simpel it is sufficient to remember that M is a direct sum of simple modules.)
- As a $\mathbb{C}[H]$-module (this is possible because $\mathbb{C}[H] \subset \mathbb{C}[G]$ is a division ring) ψ^*M is isomorphic to M. (This is the same as $i^*\psi^* = \text{id}$.)

We are going to prove that N is the kernel of the action of G on $\psi^*\mathbb{C}[H]$. We already know that $N \subset \ker(G \to \text{Aut}_{\mathbb{C}}\,\psi^*\mathbb{C}[H])$. Moreover, $\psi^*\mathbb{C}[H] \cong_{\mathbb{C}[H]} \mathbb{C}[H]$, and $H \cap \ker(G \to \text{Aut}_{\mathbb{C}}\,\psi^*\mathbb{C}[H]) = \{1\}$. Thus, $\ker(G \to \text{Aut}_{\mathbb{C}}\,\psi^*\mathbb{C}[H]) \subset N$. Hence, $N = \ker(G \to \text{Aut}_{\mathbb{C}}\,\psi^*\mathbb{C}[H])$ and $N \lhd G$. □

Chapter 13

Computing the character table

In this chapter we will compute, given a finite G (for instance by a multiplication table), the character table $[\chi(\sigma)]_{\chi\in X(G),[\sigma]\in G/\sim}$.

We know the concept of *eigenvalue* from linear algebra. Let k be a field, V be a finite-dimensional k-vector space, and $\varphi : V \to V$ be an endomorphism of V.

If λ is an element of k, the following facts are equivalent.

1. λ is an eigenvalue of φ.
2. There is $v \in V$, $v \neq 0$ such that $\varphi(v) = \lambda v$.
3. $V_\lambda = \{v \in V : \varphi(v) = \lambda v\} \neq 0$. (The *eigenspace* of φ with eigenvalue λ.)
4. $f(\lambda) = 0$, where f is the *characteristic polynomial* of φ: $f = \det(X \cdot \mathrm{id} - \varphi) \in k[X]$.
5. $V'_\lambda = \{v \in V : \exists m \geq 1 : (\lambda \cdot \mathrm{id}_V - \varphi)^m(v) = 0\} \neq 0$. (The *generalized eigenspace*.)

Let f be the characteristic polynomial of φ. If $k = \bar{k}$ (or, more generally, if $f \in k[X]$ is a product of linear factors), then $V = \bigoplus_{\lambda\in k} V'_\lambda$, and $f = \prod_{\lambda\in k}(X - \lambda)^{\dim V'_\lambda}$.

Definition 13.1 (Semisimple Endomorphism)**.** The endomorphism φ is a *semisimple endomorphism* if $V = \bigoplus_{\lambda\in k} V_\lambda$, or, equivalently, if $V_\lambda = V'_\lambda$ for all $\lambda \in k$.

Now let $k = \mathbb{C}$ and $V = Z(k[G])$. We have already seen that $V = \prod_{C\in G/\sim} k \cdot (\sum_{\sigma\in C} \sigma)$. If we define $C_i := \sum_{\sigma\in C} \sigma$ for $i = 1, \ldots, t$, we get $V = k \cdot C_1 \oplus k \cdot C_2 \oplus \cdots \oplus k \cdot C_t$.

Since V is a k-vector space and a commutative ring, for every $\alpha \in V$ there is a k-linear map $\alpha : V \to V$ given by $x \mapsto \alpha x$.

We have seen before that the isomorphism

$$Z(k[G]) \quad \xrightarrow{\sim} \quad \prod_{\chi\in X(G)} k.$$

acts on C_j by

$$C_j \quad \longmapsto \quad \left(\#C_j \frac{\chi(\sigma_j)}{\chi(1)}\right)_{\chi\in X(G).}$$

Now we give an algorithm which given G computes the character table.

1. Compute the conjugacy classes $C_1, \ldots, C_t$ of G and $\#C_i$.
2. Compute integer numbers $n_{ijk} \geq 0$ with $C_i C_j = \sum_{k=1}^{t} n_{ijk} C_k$.
3. Compute for $i = 1, \ldots, t$ the common eigenspaces of $C_1, \ldots, C_i$ and the associated eigenvalues.
4. The common eigenspaces of $C_1, \ldots, C_t$ are 1-dimensional. Call them $V_1, \ldots, V_t$ and let λ_{ij} the eigenvalue of C_i on V_j. Now if V_j belongs to χ_j and $\sigma_i \in C_i$, then $\lambda_{ij} = \#[\sigma_i]\frac{\chi_j(\sigma_i)}{\chi_j(1)}$. From the know formula

$$\sum_{\chi \in X(G)} \chi(1)\chi(\sigma) = \begin{cases} \#G \text{ if } \sigma = 1 \\ 0 \text{ if } \sigma \neq 1 \end{cases}$$

we see that

$$\frac{1}{\#[\sigma_i]} \sum_{j=1}^{t} \chi_j(1)^2 \lambda_{ij} = \begin{cases} \#G \text{ if } \sigma_i = 1 \\ 0 \text{ if } \sigma_i \neq 1 \end{cases}$$

and therefore

$$\sum_{j=1}^{t} \chi_j(1)^2 \lambda_{ij} = \begin{cases} \#G \text{ if } \sigma_i = 1 \\ 0 \text{ if } \sigma_i \neq 1. \end{cases}$$

Determine $\chi_j(1)^2$ from this linear system and define $\chi_j(\sigma_i) = \chi_j(1)\lambda_{ij}/\#[\sigma_i]$.

Example. Let $G = S_3$.

1. $C_1 = (1)$, $C_2 = (1\ 2\ 3) + (1\ 3\ 2)$, $C_3 = (1\ 2) + (1\ 3) + (2\ 3)$, $\#C_1 = 1$, $\#C_2 = 2$, $\#C_3 = 3$.
2. $C_1 = 1$, $C_2^2 = 2C_1 + C_2$, $C_3^2 = 3C_1 + 3C_2$, $C_2C_3 = 2C_3$.
3. C_1. Eigenspace $k \cdot C_1 + k \cdot C_2 + k \cdot C_3$ with eigenvalue 1.

   C_2. The multiplication by C_2 in the basis C_1, C_2, C_3 is given by the matrix $\begin{pmatrix} 0 & 2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. The characteristic polynomial of this matrix is $(X(X-1)-2)(X-2) = (X+1)(X-2)^2$. The eigenspace of C_2 with $\lambda = -1$ is $k \cdot (2C_1 - C_2)$ and the eigenspace with $\lambda = 2$ is $k \cdot (C_1 + C_2) \oplus k \cdot C_3$.

   C_3. $C_3(2C_1 - C_2) = 2C_3 - 2C_3 = 0$, and therefore C_3 has eigenvalue 0 in $(2C_1 - C_2)$. Furthermore, $C_3(C_1+C_2) = 3C_3$ and $C_3C_3 = 3(C_1+C_2)$. Thus, the multiplication by C_3 in the basis $(C_1 + C_2), C_3$ is given by the matrix $\begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}$ and the characteristic polynomial is $X^2 - 9 = (X-3)(X+3)$. The eigenspace of C_3 with $\lambda = 3$ is $k \cdot (C_1 + C_2 + C_3)$ and the eigenspace with $\lambda = -2$ is $k \cdot (C_1 + C_2 - C_3)$.
4. The eigenvalues of C_i on V_j are in the following table.

$V_j \backslash \mathbb{C}_i$	C_1	C_2	C_3
$2(C_1 - C_2)$	1	-1	0
$C_1 + C_2 + C_3$	1	2	3
$C_1 + C_2 - C_3$	1	2	-3

Now we have to solve the system

$$\chi_1(1)^2(1\ -1\ 0) + \chi_2(1)^2(1\ 2\ 3) + \chi_3(1)^2(1\ 2\ -3) = (6\ 0\ 0).$$

We get $\chi_1(1)^2 = 4$, $\chi_2(1)^2 = 1$, and $\chi_3(1)^2 = 1$. Thus, $\chi_1(1) = 2$, $\chi_2(1) = 1$, and $\chi_3(1) = 1$. This gives the character table

$\chi_j(\sigma_i)$			
	2	-1	0
	1	1	1
	1	1	-1.

Chapter 14

Induction and Brauer's theorem

Let k be a field and let $n \in \mathbb{Z}_{\geq 0}$.

Definition 14.1 (Monomial matrix)**.** An $n \times n$ matrix over k is a *monomial matrix* if it is invertible and $n(n-1)$ entries are equal to 0.

The set $\mathrm{Mon}(n,k)$ of monomial $n \times n$-matrices over k is a subgroup of $\mathrm{GL}(n,k)$.
We have the short exact sequence

$$1 \longrightarrow (k^*)^n \longrightarrow \mathrm{Mon}(n,k) \longrightarrow S_n \longrightarrow 1,$$

and the map $S_n \to \mathrm{Mon}(n,k)$ which sends σ to the permutation matrix of σ gives a splitting. We see that $\mathrm{Mon}(n,k) \cong (k^*)^n \rtimes S_n$.

Now let $k = \mathbb{C}$ and let G be a finite group. Moreover, let M be a finitely generated $k[G]$-module.

Definition 14.2 (Monomial)**.** The module M is *monomial* if there is a basis $b_1, \ldots, b_n$ of M such that

$$\forall \sigma \in G \, \forall i \in \{1, \ldots, n\} : \exists j \in \{1, \ldots, n\}, a \in k^* : \sigma b_i = a b_j$$

or, equivalently, if there exists an isomorphism $M \cong_k k^n$ such that the image of $G \to \mathrm{Aut}_k(M) \cong \mathrm{Aut}_k(k^n) \cong \mathrm{GL}(n,k)$ is contained in $\mathrm{Mon}(n,k)$.

Example. Zij $G = D_4 = \langle \rho, \sigma \rangle$.

There are four 1-dimensional simple modules and every 1-dimensional module is monomial. There is a 2-dimensional simple module. The image of ρ is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and the one of σ is $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Both are monomial matrices and therefore this simple module is also monomial.

Hence, every representation of D_4 is monomial.

Definition 14.3 (Permutation module)**.** A finitely generated $k[G]$-module is a *permutation module* if it has a k-basis which is permuted by G.

Note that a permutation module of dimension greater than 1 has a submodule which is spanned by the sum of the basis vectors.

Theorem 14.4 (Brauer's theorem)**.** *Let G be a finite group and M be a finitely generated $\mathbb{C}[G]$-module. Then there are two monomial $\mathbb{C}[G]$-modules M_1 and M_2 such that $M \oplus M_1 \cong_{\mathbb{C}[G]} M_2$.*

Corollary 14.5. *Let G be a finite group and m be the exponent of G. Then every finitely generated $\mathbb{C}[G]$-module M can be defined over $\mathbb{Q}(\zeta_m)$. That is, there exists an isomorphism $M \cong_{\mathbb{C}} \mathbb{C}^n$ such that the image of $G \to \mathrm{Aut}_{\mathbb{C}}(M) \cong \mathrm{GL}(n,\mathbb{C})$ is contained in $\mathrm{GL}(n,\mathbb{Q}(\zeta_m))$.*

In Chapter 12 we had the following diagram.

$$\begin{array}{ccccccc}
\{\text{f.g. } \mathbb{C}[G_2]\text{-modules}\}/\cong_{\mathbb{C}[G_2]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_2)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G_2/\sim} \\
\downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*\otimes \mathrm{id}} & & \downarrow{\scriptstyle (\varphi/\sim)^*} \\
\{\text{f.g. } \mathbb{C}[G_1]\text{-modules}\}/\cong_{\mathbb{C}[G_1]} & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1) & \hookrightarrow & \mathcal{R}_{\mathbb{C}}(G_1)\otimes_{\mathbb{Z}}\mathbb{C} & \cong & \mathbb{C}^{G_1/\sim}.
\end{array}$$

We can also construct the map φ_*. Note that $\varphi_*(M) = k[G_2] \otimes_{k[G_1]} M$ is a $k[G_2]$-module, because $k[G_2]$ is a $k[G_2]$-$k[G_1]$-bimodule.

In the special case where $G_1 = H$ is a subgroup of $G_2 = G$ and $\varphi = i$ is the inclusion map $H \subset G$, we also call i_* *induction* from H to G and we denote it by Ind_H^G.

Now let G be a finite group, $H \subset G$ be a subgroup and M be a $k[H]$-module. How does $\mathrm{Ind}_H^G M = k[G] \otimes_{k[H]} M$ look like?

Write $G = \coprod_{\rho \in P} \rho H$. Then $k[G] = \bigoplus_{\rho \in P} \rho \cdot k[H]$. It follows that $k[G] \otimes_{k[H]} M = \bigoplus_{\rho \in P} \rho \cdot M$. If $\sigma \in G$, $x \in M$ and $\rho \in P$, there are a $\rho' \in P$ and a $\tau \in H$ such that $\sigma\rho = \rho'\tau$. From this we see that $\sigma(\rho x) = \rho'(\tau x) \in \rho' \cdot M$.

Example. If $M = k$, then $\mathrm{Ind}_H^G k$ is a permutation module with underlying vector space $k^{G/H}$.

A finitely generated $k[G]$-module N is monomial if and only if N is of the form $\bigoplus_{i=1}^r \mathrm{Ind}_{H_i}^G(M_i)$, with $H_i \subset G$ a subgroup and M_i a 1-dimensional $k[H_i]$-module.

Bibliography

[1] Helmut Bender and George Glauberman. *Local analysis for the odd order theorem*, volume 188 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1994. With the assistance of Walter Carlip.

[2] Thomas Peterfalvi. *Character theory for the odd order theorem*, volume 272 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Translated from the 1986 French original by Robert Sandling and revised by the author.