Graduate Algebra

Diane Maclagan
Notes by Florian Bouyer

Contents

1 Introduction

1.1 Groups

Definition 1.1. A *semigroup* is a non-empty set G together with a binary operation ("multiplication") which is associative ($(ab)c = a(bc)\,\forall a, b, c \in G$)

A *monoid* is a semigroup G which contains an element $e \in G$ such that $ae = ea = a\,\forall a \in G$.

A *group* is a monoid such that $\forall a \in G\,\exists a^{-1}$ such that $aa^{-1} = a^{-1}a = e$.

Note. Many authors say "semigroup" for monoid. e.g. $\mathbb{N} = \{0, 1, \dots\}$ is called a semigroup.

Example (Semigroups that are not monoids)**.**

- A proper ideal in a ring under multiplication
- $(\mathbb{N} \setminus \{0\}, +)$
- $(2\mathbb{Z}, \times)$
- $(M_n(2\mathbb{Z}), \times)$
- $(\mathbb{R}, \min)$

Example (Monoids that are not groups)**.**

- $(\mathbb{N}, +)$
- Polynomials in 1 variable under composition
- Rings with identity that has non-invertible elements under multiplication
- $(\mathbb{R} \cup \infty, \min)$

Exercise.

- In a monoid, identities are unique
- In a group, inverses are unique.

Definition 1.2. Let G and H be semigroups. A function $f : G \to H$ is a *homomorphism of semigroups* if $f(ab) = f(a)f(b)\,\forall a, b \in G$

If it is a bijection, it is called an *isomorphism*.

Let G and H be monoids. A *monoid homomorphism* is a semigroup homomorphism with $f(e_G) = e_H$

A *group homomorphism* between groups G, H is a semigroup homomorphism between the underlying semigroups.

Group homomorphisms are automatically monoid homomorphisms: $f : G \to H$, $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$. Multiply by $f(e_G)^{-1}$ then we get $e_H = f(e_G)^{-1}f(e_G) = f(e_G)^{-1}f(e_G)f(e_G) = e_H f(e_G) = f(e_G)$.

Example (Important example of a group: Permutation Group)**.** Let X be a non-empty set. Let $P(X)$ be the set of all bijection $f : X \to X$. $P(X)$ is a group under function composition that is $fg : X \to X$ is $f \circ g : X \to X$.

- This is associative because function composition is
- The identity is id (the identity map)
- The inverse of f is $f^{-1} : X \to X$. (Which exists since f is a bijection

If $|X| = n$ then $P(X) \cong S_n$ (the symmetric group on n elements)

Definition 1.3. A *sub{group, monoid, semigroup}* of a {group, monoid, semigroup} G is a subset $H \subset G$ that is a {group, monoid, semigroup} under the operation of G.

Let $\phi : G \to H$ be a group homomorphism, the *kernel of* ϕ is $\ker\phi = \{a \in G | \phi(a) = e_H\}$

Note. The kernel of ϕ is a subgroup of G. In fact it is <u>normal </u>(i.e., $\forall g \in G$, $ghg^{-1} \in H = \ker\phi$ for all $h \in H\}$

Definition 1.4. A group G is *abelian* if $ab = ba$ for all $ab \in G$

Exercise. Find $\phi : G \to H$ (G, H monoid) that is a semigroup homomorphism but not a monoid homomorphism

$(\mathbb{R}, \times) \to (M_2(\mathbb{R}), \times)$ by $\phi(a) \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

1.2 Rings

Definition 1.5. A *ring* R is a non-empty set R together with binary operations $+, \times$ such that

1. $(R, +)$ is an abelian group (write identity as 0)

2. $a(bc) = (ab)c$ (multiplication is associative, so $(R, \times)$ is a semigroup)

3. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (distributivity)

If there is $1_R \in R$ such that $1_R a = a 1_R = a \, \forall a \in R$ then R is a ring *with identity*

R is *commutative* if $ab = ba \, \forall a, b \in R$.

Let R, S be rings. A ring *homomorphism* $\phi : R \to S$ is a function ϕ such that :

1. $\phi(r + s) = \phi(r) + \phi(s)$ (group homomorphism)

2. $\phi(rs) = \phi(r)\phi(s)$ (semigroup homomorphism)

Note. We do not require that if R, S have identities, that $\phi(1_R) = 1_S$ (e.g., $\phi(a) = 0_S \, \forall a$ is OK)

Definition 1.6. Let R be a ring with identity. An element $a \in R$ is *left* (respectively *right*) *invertible* if $\exists b \in R$ (respectively $c \in R$) such that $ba = 1_R$ (respectively $ac = 1_R$)

If a is left and right invertible then a is called *invertible*, or a *unit*.

A ring with identity $1_R \neq 0_R$ in which every non-zero element is a unit is a *division ring*. A commutative division ring is a *field*.

A field homomorphism is a ring homomorphism ϕ of the underlying rings.

Example (Useful example of a ring: Group rings)**.** Let R be a commutative ring with 1. Let G be a group. The group ring $R[G]$ has entries $\left\{\sum_{g \in G} r_g g : r_g \in R\right\}$ "formal sums" (all but finitely many $r_g = 0$). This is a ring under coordinate wise addition, and multiplication is induced from $(g_1)(g_2) = (g_1 g_2)$.

e.g.: $R = \mathbb{C}, G = \mathbb{Z}$ then $\mathbb{C}[\mathbb{Z}] = \mathbb{C}[t, t^{-1}]$. $\mathbb{C}[\mathbb{Z}/3\mathbb{Z}] = \mathbb{C}[t]/(t^3)$

Definition 1.7. Let R be a ring. A (*left*) R-*module* is an abelian group M (write additively) together with a function $R \times M \to M$ such that

1. $r(m + m') = rm + rm'$

2. $(r + s)m = rm + sm$

3. $r(sm) = (rs)m$

If R is a field an R-module is a vector space. If R has 1_R we usually ask $1_R m = m$ for all $m \in M$.

Definition 1.8. An R-module *homomorphism* is a group homomorphism $\phi : M \to M'$ such that $\phi(rm) = r\phi(m)$.

2 Category Theory

Definition 2.1. A *category* is a class $\mathrm{Ob}(\mathscr{C})$ of objects (write $A, B, C, \ldots$) together with:

1. a class, $\mathrm{mor}(\mathscr{C})$, of disjoint sets $\hom(A, B)$. one for each pair of objects in $\mathrm{Ob}(\mathscr{C})$. An element f of $\hom(A, B)$ is called a *morphism* from A to B. (write $f : A \to B$)
2. For each triple (A, B, C) of objects: a function $\hom(B, C) \times \hom(A, B) \to \hom(A, C)$ (write $(f, g) \mapsto f \circ g$) "composition of morphism satisfying:
   (a) associativity: $h \circ (g \circ f) = (h \circ g) \circ f$ with $f \in \hom(A, B)$, $g \in \hom(B, C)$ and $h \in \hom(C, D)$
   (b) Identity: For each $B \in \mathrm{Ob}(\mathscr{C})$ there exists $1_B : B \to B$ such that $\forall f \in \hom(A, B)$ $1_B \circ f = f$ and $\forall g \in \hom(B, C)$ $g \circ 1_B = g$

Example.

Sets: Objects: the class of all sets. Morphisms $\hom(A, B)$ is the set of all functions $f : A \to B$

Groups: Objects: Groups. Morphisms: group homomorphism.

Semigroups: Object: semigroups. Morphisms: semigroup homomorphism

Monoids: Object: monoids. Morphisms: monoid homomorphism.

Rings: Objects: Rings. Morphisms: ring homomorphism

Ab: Objects: abelian groups. Morphisms: group homomorphism

Vect_k: Objects: Vector spaces over (a field) k. Morphisms: linear transformations.

Top: Objects: Topological spaces. Morphisms: Continuous functions.

Manifolds: Objects: Manifolds. Morphisms: Continuous maps.

Diff: Objects: Differentiable manifolds. Morphisms: differentiable maps

Point Let G be a group. Object: one point. Morphisms: $\hom(\mathrm{pt}, \mathrm{pt}) = G$ (composition is multiplication)
Note. $\forall f \in \hom(\mathrm{pt}, \mathrm{pt})$ there exists g such that $f \circ g = 1_{\mathrm{pt}} = g \circ f$. (This example is useful for Groupoid)

Open Sets Fix a topological space X. The category of open set on X: Objects: Open sets. Morphisms: inclusions. (i.e., $\hom(A, B)$ is empty or has size one) (This example is useful for sheaves)

R-module Fix a ring R. Objects: are R-modules. Morphisms: R-module homomorphism $\phi(rm) = r\phi(m)$

Definition 2.2. In a category a morphism $f \in \hom(A, B)$ is called an *equivalence* if there exists $g \in \hom(B, A)$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

If $f \in \hom(A, B)$ is an equivalence then A and B are said to be *equivalent.*

Example. Groups Equivalence is isomorphism

Top Equivalence is homeomorphism

Set Equivalence is bijection.

Definition 2.3. Let $\mathscr{C}$ be a category and $\{A_\alpha : \alpha \in I\}$ be a family of objects of $\mathscr{C}$. A *product* for the family is an object P of $\mathscr{C}$ together with a family of morphisms $\{\pi_\alpha : P \to A_\alpha : \alpha \in I\}$ such that for <u>any</u> object B with morphisms $\phi_\alpha : B \to A_\alpha$ $\exists! \phi : B \to P$ such that $\phi_\alpha \circ \phi = \phi_\alpha \, \forall \alpha$

Example. $|I| = 2$

$$\begin{tikzcd}
& B \arrow[d, dashed, "\exists!"] \arrow[ddl, "\phi_1"'] \arrow[ddr, "\phi_2"] & \\
& P \arrow[dl, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
A_1 & & A_2
\end{tikzcd}$$

Warning: Products don't always exists, but when they do, we often recognize them

Example.

Set: Products is Cartesian product.

Groups Product is direct product.

Open sets of X Interior $(\cap A_\alpha)$.

Lemma 2.4. *If (P, π_α) and (Q, ψ_α) are both products of the family $\{A_\alpha, \alpha \in I\}$ then P and Q are equivalent (isomorphic).*

Proof. Since Q is a product $\exists! f : P \to Q$ such that $\pi_\alpha = \psi_\alpha \circ f$. Since P is a product $\exists! g : Q \to P$ such that $\psi_\alpha = \pi_\alpha \circ g$. So $g \circ f : P \to P$ satisfies $\pi_\alpha = \pi_\alpha \circ (g \circ f)\, \forall \alpha$. Since P is a product $\exists! h : P \to P$ such that $\pi_\alpha = \pi_\alpha \circ h$. Since $h = 1_P$ satisfies this, we must have $g \circ f = 1_P$. Similarly $f \circ g : Q \to Q$ equals 1_Q. So f is an equivalence. $\square$

Definition 2.5. An object I in a category $\mathscr{C}$ is *universal* (or initial) if for all objects $C \in \mathrm{Ob}(\mathscr{C})$ there is an unique morphism $I \to C$. J is *couniversal* (or terminal) if for all object C there is a unique morphism $C \to J$.

Example.

Sets $\emptyset$ initial, $\{x\}$ terminal.

Groups Trivial group, initial and terminal.

Open sets $\emptyset$ is initial. X is terminal

Example. Pointed topological spaces: Objects: Pairs (X, p) where X is a non-empty topological space, $p \in X$. Morphisms: Continuous maps $f : (X, p) \to (Y, q)$ with $f(p) = q$. $(\{p\}, p)$ is terminal and initial.

Theorem 2.6. *Any two initial (terminal) objects in a category are equivalent.*

Proof. Let I, J be two initial objects in $\mathscr{C}$. Since I is initial $\exists! f : I \to J$. Since J is initial $\exists! g : J \to I$. Since I is initial, 1_I is the only morphism $I \to I$, so $g \circ f = 1_I$. Similarly, $f \circ g = I_J$ so f is an equivalence. For terminal objects the proof is the same with the arrows reversed. $\square$

Why is the lemma a special case of the theorem. Let $\{A_\alpha : \alpha \in I\}$ be a family of objects in a category $\mathscr{C}$. Define a category $\mathscr{E}$ whose objects are all pairs $(B, f_\alpha : \alpha \in I)$ where $f_\alpha : B \to A_\alpha$. The morphisms are morphisms $(B, f_\alpha) \to (C, g_\alpha)$ are morphisms $h : B \to C$ such that $f_\alpha = g_\alpha \circ h$.

Check:

- $I_B : B \to B$ induces $1_{(B, f_\alpha)}$in $\mathscr{E}$
- Composition of morphisms is still ok (These first two checks that $\mathscr{E}$ is a category)
- h is an equivalence in $\mathscr{E}$ implies h is an equivalence in $\mathscr{C}$. (This will help us show what we wanted)

If a product of $\{A_\alpha\}$ exists, it is terminal in $\mathscr{E}$. We just showed terminal objects are unique (up to equivalence) so products are unique (up to equivalence).

Note. Not every category has products. (for example finite groups)

Definition 2.7. A *coproduct* of $\{A_\alpha\}$ in $\mathscr{C}$ is "a product with the arrows reversed", i.e., Q with $\pi_\alpha : A_\alpha \to Q$ such that $\forall C$ with $\phi_\alpha : A_\alpha \to C$, $\exists! f : Q \to C$ such that $\phi_\alpha = f \circ \pi_\alpha$

$$\begin{tikzcd}
A_1 \arrow[dr, "\pi_1"] \arrow[ddr, "\phi_1"'] & & A_2 \arrow[dl, "\pi_2"'] \arrow[ddl, "\phi_2"] \\
& Q \arrow[d, dashed, "\exists!"] & \\
& C &
\end{tikzcd}$$

Example. The coproduct of sets is a disjoint union.

For the pointed topological space we have the product is $(\prod X_\alpha, \prod p_\alpha)$. The coproduct is the wedge product, that is, (in the case of the coproduct of two object) $X \coprod Y / p \sim q$.

For abelian groups the coproduct is direct sum, i.e., $\oplus_I G_\alpha \ni (g_\alpha : \alpha \in I, g_\alpha \in G_\alpha)$ and all but finitely many $g_\alpha = e_{G_\alpha}$.

2.1 Functors

Definition 2.8. Let $\mathscr{C}$ and $\mathscr{D}$ be categories. A *covariant* functor T from $\mathscr{C}$ to $\mathscr{D}$ is a pair of functions (both denoted by T):

1. An object function: $T : \mathrm{Ob}(\mathscr{C}) \to \mathrm{Ob}(\mathscr{D})$
2. A morphism function $T : \mathrm{mor}(\mathscr{C}) \to \mathrm{mor}(\mathscr{D})$ with $f : A \to B \mapsto T(f) : T(A) \to T(B)$ such that
   (a) $T(1_C) = 1_{T(C)} \forall C \in \mathrm{Ob}(\mathscr{C})$
   (b) $T(g \circ f) = T(g) \circ T(f)$ for all $f, g \in \mathrm{mor}(\mathscr{C})$ where composition is defined

Example.
- The "forgetful functor" from Groups to Sets. $T(G)$ =underlying set and $T(f) = f$ (i.e. same functions, thought of as a map of sets)
- $\hom(G, -)$:Groups$\to$Sets. Let G be a fixed group. Let T be the functor that takes a group H to the set $\hom(G, H)$. If $f : H \to H'$ is a group homomorphism, then $T(f) : T(H) \to T(H')$ is given by $T(f)(g) = f \circ g$.

  Check:
  - $T(1_H)(g) = 1_H \circ g = g$ so $T(1_H) = 1_{T(H)}$
  - $T(g \circ f)(h) = (g \circ f) \circ h = g \circ (f \circ h) = T(g)(f \circ h) = T(g)(T(f)(h)) = (T(g) \circ T(f))(h)$

Definition 2.9. Let $\mathscr{C}$ and $\mathscr{D}$ be categories. A *contravariant* functor T from $\mathscr{C}$ to $\mathscr{D}$ is a pair of functions (both denoted by T):

1. An object function: $T : \mathrm{Ob}(\mathscr{C}) \to \mathrm{Ob}(\mathscr{D})$
2. A morphism function $T : \mathrm{mor}(\mathscr{C}) \to \mathrm{mor}(\mathscr{D})$ with $f : A \to B \mapsto T(f) : T(B) \to T(A)$ such that
   (a) $T(1_C) = 1_{T(C)} \forall C \in \mathrm{Ob}(\mathscr{C})$
   (b) $T(g \circ f) = T(f) \circ T(g)$ for all $f, g \in \mathrm{mor}(\mathscr{C})$ where composition is defined

Example. $\hom(-, G)$:Groups$\to$Sets. Let G be a fixed group. Let T be the functor that takes a group H to the set $\hom(H, G)$. If $f : H \to H'$ is a group homomorphism, then $T(f) : T(H') \to T(H')$ is given by $T(f)(g) = g \circ f$.

Definition 2.10. Let $\mathscr{C}$ be a category. The *opposite category* $\mathscr{C}^{\mathrm{op}}$ has object $\mathrm{Ob}(\mathscr{C})$ and $\hom_{\mathscr{C}^{\mathrm{op}}}(A, B) = \hom_{\mathscr{C}}(B, A)$. ("reverse the arrows")

One can see that this is a category with $g^{\mathrm{op}} \circ f^{\mathrm{op}} = (f \circ g)^{\mathrm{op}}$.
If $T : \mathscr{C} \to \mathscr{D}$ is a contravariant functor then $T^{\mathrm{op}} : \mathscr{C}^{\mathrm{op}} \to \mathscr{D}$ defined by $T^{\mathrm{op}}(C) = T(C)$ and $T^{\mathrm{op}}(f) = T(f)$ is covariant.

2.2 Some natural occurring functors

1. Fundamental group (ref: Hatcher "Algebraic Topology")

   π_1 : Pointed topological spaces $\to$Groups. $\pi_1(X, p)$ =homotopy classes of maps $f : [0, 1] \to X$ such that $f(0) = f(1) = p$. This is a group under concatenation of loops. $f \circ g : [0, 1] \to X$ with $f \circ g(t) = \begin{cases} g(2t) & 0 \le t \le \frac{1}{2} \\ f(2t-1) & \frac{1}{2} \le t \le 1 \end{cases}$, $f^{-1}(t) = f(1-t)$. If $\phi : (X, x) \to (Y, y)$ is a continuous map with $\phi(x) = y$, then we get an induced map $\pi_1(X, x) \to \pi_1(Y, y)$ by $(f : [0, 1] \to X) \mapsto (\phi(f) : [0, 1] \to Y)$ by $\phi(f)(t) = \phi \circ f(t)$.

   Check:
   (a) This is a group homomorphism
   (b) $\pi_1(1_{(X,x)}) = 1_{\pi_1(X,x)}$
   (c) $\pi_1(\phi \circ \psi) = \pi_1(\phi) \circ \pi_1(\psi)$

   Recall: A group is a category with one object where all morphisms are isomorphisms (have inverses). A groupoid is a category where all morphisms are isomorphisms.

2. Consider the category $\mathscr{U}(X)$ of open sets on X with morphisms inclusion $T : \mathscr{U} \to$Sets, $T(U) = \{$continuous functions from U to $\mathbb{R}\}$. If $V \subseteq U$ then $T(V) \leftarrow T(U)$ (by restriction). Good easy exercise is to finish checking that this is a functor. This is an example of a presheaf.

2.3 Natural Transformations

Definition 2.11. Let $\mathscr{C}$ and $\mathscr{D}$ be categories and let S and T be covariant functors from $\mathscr{C}$ to $\mathscr{D}$. A *natural transformation* α from S to T is a collection $\{\alpha_c : c \in \mathrm{Ob}(\mathscr{C})\}$ in $\mathrm{mor}(\mathscr{D})$, where $\alpha_c : S(C) \to T(C)$ such that if $f : C \to C'$ is a morphism in $\mathscr{C}$ then

$$\begin{tikzcd} S(C) \arrow[r, "\alpha_c"] \arrow[d, "S(f)"'] & T(C) \arrow[d, "T(f)"] \\ S(C') \arrow[r, "\alpha_{c'}"] & T(C') \end{tikzcd}$$

commutes.

Example. $\mathscr{C}$ =groups, $\mathscr{D}$ =sets. $S = \hom(G, -)$ and $T = \hom(H, -)$. Let $\phi : H \to G$ be a group homomorphism. Given a group A, we construct $\alpha_A : \hom(G, A) \to \hom(H, A)$ by $g \mapsto g \circ \phi$ (where $\phi : H \to G$). Let $f : A \to B$

$$\begin{tikzcd} \hom(G, A) \arrow[r, "g \mapsto g\circ\phi"] \arrow[d, "g \mapsto f \circ g"'] & \hom(H, A) \arrow[d, "g' \mapsto f \circ g'"] \\ \hom(G, B) \arrow[r, "g' \mapsto g \circ \phi"] & \hom(H, B) \end{tikzcd}$$

Definition 2.12. A natural transformation where all α_c are isomorphism is called a *natural isomorphism.*

Example. Let $\mathscr{C} = \mathscr{D} =n$-dimensional vector space over k. Let $S =$ id and $T : V \to V^{**}$ (i.e. $T(V) = V^{**}$ if $f : V \to W, w^* \to k$ then $T(f) : V^{**} \to W^*$, $T(f)(\beta) \in W^{**}$ we have $T(f)(\beta)(\psi) = \beta(\psi \circ f) \in k$

We claim T and S are naturally isomorphic. For $V \in \mathrm{Vect}_n^k$, let α_v be the linear transformation $V \to V^{**}$ given by $v \mapsto \phi_V$ where $\phi_V(\psi) = \psi(v)$. Then for $f : V \to W$

$$\begin{tikzcd} V \arrow[r, "\alpha_V"] \arrow[d, "S(f)=f"'] & V^{**} \arrow[d, "T(f)"] \\ W \arrow[r, "\alpha_W"] & W^{**} \end{tikzcd}$$

$$\begin{aligned} T(f)(\alpha_V(v))(\psi) &= T(f)(\phi_V)(\psi) \\ &= \phi_V(\psi \circ f) \\ &= \psi \circ f(v) \\ &= \phi_{f(v)}(\psi) \end{aligned}$$

Since $\alpha_w \circ f(v) = \phi_{f(v)}$ means the diagram commutes. Since each α_V is an isomorphism (exercise that this uses finite dimension), T is naturally isomorphic to S.

Definition. Two categories $\mathscr{C}$ and $\mathscr{D}$ are equivalent if there are functors $f : \mathscr{C} \to \mathscr{D}$ and $g : \mathscr{D} \to \mathscr{C}$ such that $f \circ g$ is natural isomorphic to $1_{\mathscr{D}} : \mathscr{D} \to \mathscr{D}$, $g \circ f$ is naturally isomorphic to $1_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$.

3 Free Groups

Intuitive idea: Group formed by "words" in an alphabet. Multiplication is concatenation, e.g. F_2 =words in x and y for example $xyx^{-1}y^{-1}x^3y^2$

Construction

Input: A set X (might be infinite)

1) Choose a set X^{-1} disjoint from X with $|X^{-1}| = |X|$ and a bijection $X \to X^{-1}$, $x \mapsto x^{-1}$. Choose an element $1 \notin X \cup X^{-1}$

2) A *word* on X is a sequence $(a_!, a_2, \dots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ such that there exists N such that $a_n = 1 \forall n > N$. $(1, 1, 1, \dots)$ is the empty word and written as 1

3) A word is *reduced* if:

   1. $\forall x \in X$, x and x^{-1} are never adjacent (i.e., if $a_k = x$ then $a_{k-1}, a_{k+1} \neq x^{-1}$)
   2. $a_k = 1 \Rightarrow a_i = 1 \forall i > k$

   A non-empty reduced word has the form $(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, 1, 1, \dots)$ with $x_i \in X$ and $\lambda_i = \pm 1$. Write this as $x_1^{\lambda_1}x_2^{\lambda_2}\dots x_n^{\lambda_n}$.

4) Our group $F(X)$ as a set is the set of reduced words.
   Naive attempt at defining multiplication: Define $(x_1^{\lambda_1}\dots x_n^{\lambda_n})(y_1^{\delta_1}\dots y_m^{\delta_m})$ to be $x_1^{\lambda_1}\dots x_n^{\lambda_n}y_1^{\delta_1}\dots y_m^{\delta_m}$
   Problem: This product might not be reduced
   Solution: Reduce it:
   Formally: if $a = (x_1^{\lambda_1}\dots x_m^{\lambda_m})(y_1^{\delta_1}\dots y_n^{\delta_n})$ (and suppose that $m \leq n$). Let $K = \max_{0 \leq k \leq n}\{k : x_{m-j}^{\lambda_{m-j}} = y_{j+1}^{-\delta_j+1} \text{ for all } 0 \leq j \leq k-1\}$. Then define
   $$ab = \begin{cases} x_1^{\lambda_1}\dots x_{m-k}^{\lambda_{m-k}}y_{k+1}^{\delta_{k+1}}\dots y_n^{\delta_n} & k < m \\ y_{m+1}^{\delta_{m+1}}\dots \delta_n^{\delta_n} & k = m < n \text{ (and analogously if } m > n) \\ 1 & k = m = n \end{cases}$$
   This define a multiplication $F(X) \times F(X) \to F(X)$.
   Claim: This is a group

   - 1 is the identity
   - The inverse of $x_1^{\lambda_1}\dots x_m^{\lambda_m}$ is $x_m^{-\lambda_m}\dots x_1^{-\lambda_1}$
   - For associativity see Lemma 3.1

Lemma 3.1. *The multiplication $F(X) \times F(X) \to F(X)$ is associative.*

Proof. For each $x \in X$ and $\delta = \pm 1$ let $|x^\delta| : F(X) \to F(X)$ be the map given by:

- $1 \mapsto x^\delta$
- $x_1^{\delta_1}\dots x_n^{\delta_n} \mapsto \begin{cases} x^\delta x_1^{\delta_1}\dots x_n^{\delta_n} & x^\delta \neq x_1^{-\delta_1} \\ x_2^{\delta_2}\dots x_n^{\delta_n} & x^\delta = x_1^{-\delta_1}, n > 1 \\ 1 & n = 1, x^\delta = x^{-\delta_1} \end{cases}$

Note that this map is a bijection, since $|x^\delta||x^{-\delta}| = 1 = |x^{-\delta}||x^\delta|$. Let $A(X)$ be the group of all permutations of $F(X)$. Consider the map $\phi : F(X) \to A(X)$ given by

- $1 \mapsto 1_{A(X)}$
- $x_1^{\delta_1}\dots x_n^{\delta_n} \mapsto |x_1^{\delta_1}||x_2^{\delta_2}|\dots|x_n^{\delta_n}|$

since $|x_1^{\delta_1}|\dots|x_n^{\delta_n}| : 1 \mapsto x_1^{\delta_1}\dots x_n^{\delta_n}$ we have ϕ is injective. Note that if $w_1, w_2 \in F(X)$, then $\phi(w_1w_2) = \phi(w_1)\phi(w_2)$. Since $A(X)$ is a group, the multiplication is associative, so the multiplication in $F(X)$ is associative. □

Example.

- $X = \{x\}$, $F(X) \cong \mathbb{Z}$ (reduced words are $1, x^n, x^{-n}$)

- $X = \{x, y\}$. $F(X) =$"words in x, y, x^{-1}, y^{-1}, e.g. $xyx^{-1}y^{-1}$ is reduced. So $F(X)$ is not abelian as $xyx^{-1}y^{-1} \neq 1$ so $xy \neq yx$.

Note. There is an inclusion $i : X \to F(X)$.

Lemma 3.2. *If G is a group and $f : X \to G$ is a map of sets then $\exists!$ homomorphism $\overline{f} : F(X) \to G$ such that $\overline{f}i = f$.*

Proof. Define $\overline{f}(1) = e \in G$. If $x_1^{\delta_1} \dots x_n^{\delta_n}$ is a non-empty reduced word on X, set $\overline{f}(x_1^{\delta_1} \dots x_n^{\delta_n}) = f(x_1)^{\delta_1} \dots f(x_n)^{\delta_n}$. Then $\overline{f}$ is a group homomorphism with $\overline{f}i = f$ by construction and it is unique by the homomorphism requirement. $\square$

This says the free group is a free object in the category of group. If $\mathscr{C}$ is a concrete category (there exists a forgetful functor $F : \mathscr{C} \to$Sets) and $i : X \to F(X)$, where X is a set and $A \in \mathrm{Ob}(\mathscr{C})$, is a function, then A is free on X if for all $j : X \to F(B)$ $\exists!$ $\phi : A \to B$ such that $\phi \circ i = j$. (Note $B \in \mathrm{Ob}(\mathscr{C})$ and $\phi \in \mathrm{mor}(\mathscr{C})$).

Compare:

- Vector Spaces
- Commutative k-algebra
- R-modules

Corollary 3.3. *Every group G is the homomorphic image of the a free group.*

Proof. Let X be a set of generators of G.The inclusion $f : X \to G$ gives a map $\overline{f} : F(X) \underset{x \mapsto x}{\to} G$. The map $\overline{f}$ is surjective since X is a set of generators. So $G \cong F(X)/\ker(f)$. $\square$

Definition 3.4. Let G be a group and let Y be a subset of G. The *normal subgroup* $N = N(Y)$ of G generated by Y is the intersection of all normal subgroups of G containing Y.

Check that it is well defined. (That is check $N(Y)$ is non-empty, it relies on the fact G is normal)

Definition 3.5. Let X be a set and let Y be a set of (reduced) words on X. A group G is said to be *defined by generators X and relations* $w = e$ for $w \in Y$ if $G \cong F(X)/N(Y)$. (We say $(X|Y)$ is a *presentation* of G)

Example. $\langle x | x^6 \rangle \cong \mathbb{Z}/6\mathbb{Z}$
$\langle x, y | x^4, y^2, (xy)^2 \rangle \cong D_4$ (or D_8 depending of your notation)

Note. Presentations are not unique, e.g., $\langle x, y | x^3, y^2, xyx^{-1}y^{-1} \rangle \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\langle x, y | xy^{-5} \rangle \cong \mathbb{Z}$, $\langle x, y | x^2, y^2, (xy)^4 \rangle \cong D_4$ (the Coveter presentation)

Given a presentation $G = \langle X | R \rangle \cong F(X)/N(R)$. The word problem asks if a given word $w \in F(X)$ equals the identity of G. This is undecidable! [Novikav 1955].

Example. Burnside groups, $B(m, n) = \langle x_1, \dots, x_m | w^n$ for any word $w\rangle$. Question (Burnside 1902) Is $B(n, m)$ finite? In the case $B(1, n) \cong \mathbb{Z}/n\mathbb{Z}$ and $B(m, 2) \cong (\mathbb{Z}/2\mathbb{Z})^n$.

Question: What are free objects in the category of abelian groups? $\bigoplus_{x \in X} \mathbb{Z}$.

4 Tensor Product

We'll work in the category of R-modules (no assumptions are made on R, including whether it has 1 or not). (Cross-reference this whole chapter with Commutative Algebra Chapter 2)

Recall M is a *left* R-module if $R \times M \to M$ with $(r,m) \mapsto rm$ and $r(s(m)) = (rs)m$. And M is a *right* R-module if $R \times M \to M$ with $(r,m) \mapsto mr$ and $(mr)s = m(rs)$

Example. $R = M_n(\mathbb{C})$ and $M = \mathbb{C}^n$ is left (M is columns vectors) or right (M is row vectors) R-module

If R is commutative a left R-module structure gives rise to a right R-module structure, i.e., we define $mr = rm$. M is an $S-R$ bimodule if M is a left S-module and a right R-module and $(sm)r = s(mr)$, e.g., $\mathbb{C}^n$ is a $M_n(\mathbb{C}) - \mathbb{C}$ bimodule.

Suppose we have $f : A \oplus B \to C$ such that $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$, $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$ and $f(ar, b) = f(a, rb)$. We show $A \times B \to A \otimes_R B \to C$.

Example. $f : \mathbb{R}^2 \oplus \mathbb{R}^2 \to \mathbb{R}$, $f\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}\right) = 4ac + bc + ad + 4bd$. (Easy to check the above relations holds)

Definition 4.1. Let A be a right R-module and B a left R-module. Let F be the free abelian group on the set $A \times B$. Let K be the subgroup generated by all elements:

1. $(a + a', b) - (a, b) - (a', b)$
2. $(a, b + b') - (a, b) - (a, b')$
3. $(ar, b) - (a, rb)$

for all $a, a' \in A, b, b' \in B$ and $r \in R$. The quotient F/K is called the *tensor product* of A and B and is written $A \otimes_R B$. Note: $(a, b) + K$ is written $a \otimes b$ and $(0, 0) + K$ is written 0. This is an abelian group.

Warning: Not every element of $A \otimes_R B$ has the form $a \otimes b$. A general element is (finite) $\sum n_i (a_i \otimes b_i)$ with $n_i \in \mathbb{Z}$.

We have relations $(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b$, $a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2$ and $ar \otimes b = a \otimes rb$. If A is a $S-R$ bimodule then $A \otimes_R B$ is a left S-module since F is an S-module by $s(a, b) = (sa, b)$ and K is an S-submodule.

Example. $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. (c.f. Commutative Algebra)

There is a function $\pi : A \times B \to A \otimes_R B$ defined by $(a, b) \mapsto a \otimes b$. Note: π is not a group homomorphism as $(a_1 + a_2, b_1 + b_2) \mapsto a_1 \otimes b_1 + a_1 \otimes b_2 + a_2 \otimes b_1 + a_2 \otimes b_2$. However $\pi(a_1 + a_2, b) = \pi(a_1, b) + \pi(a_2, b)$ and $\pi(a, b_1 + b_2) = \pi(a, b_1) + \pi(a, b_2)$ and $\pi(ar, b) = \pi(a, rb)$. (Call these relations "middle linear")

The universal property of Tensor Product . *Let $A_R, {}_R B$ be R-module and C an abelian group. If $g : A \times B \to C$ is "middle linear" then $\exists! \overline{g} : A \otimes_R B \to C$ such that $\overline{g}\pi = g$.*

$$\begin{tikzcd}
A \times B \arrow[d, "\pi"'] \arrow[dr, "g"] & \\
A \otimes_R B \arrow[r, dashed, "\exists!"'] & C
\end{tikzcd}$$

If A is an $S - R$ bimodule and C is an S-module then $\overline{g}$ is a S-module homomorphism.

Proof. Let F be the free abelian group on $A \times B$. There is a unique group homomorphism $g_1 : F \to C$ determined by $(a, b) \mapsto g(a, b)$. Since g is "middle linear", $g_1((a + a', b) - (a, b) - (a', b)) = g(a + a', b) - g(a, b) - g(a', b) = 0$. Similarly, the other generators of Klive in $\ker g_1$, so we get an induced map $\overline{g} : \underbrace{A \otimes_R B}_{=F/K} \to C$. Note that $\overline{g}(a \otimes b) = g_!((a, b)) = g(a, b)$ so $\overline{g}\pi = g$.

If $h : A \otimes B \to C$ is a group homomorphism with $h\pi = g$ then $h(a \otimes b) = h\pi(a, b) = g(a, b) = \overline{g}(\pi(a, b)) = \overline{g}(a \otimes b)$. So h and $\overline{g}$ agree on generators $a \otimes b$ of $A \otimes_R B$, so $h = \overline{g}$. $\square$

Example. $R = \mathbb{Z}, A = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}$, $B = \mathbb{Q}$. Then $A \otimes_R B = \mathbb{Q}$.

To prove this, define $f : \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z} \times \mathbb{Q} \to \mathbb{Q}$ by $f((a,b),c) = bc$. Then $f((a_1,b_1)+(a_2,b_2),c) = b_1c + b_2c = f((a_1,b_1),c) + f((a_2,b_2),c)$, $f((a,b),c_1+c_2) = b(c_1+c_2) = bc_1 + bc_2$, $f((a,b)n,c) = f((na,nb),c) = nbc = f((a,b),nc)$. So f is "middle linear", so by the proposition there exists a unique $\overline{f} : A \otimes B \to \mathbb{Q}$ with $\overline{f}((a,b) \otimes c) = bc$. We have that $\overline{f}$ is surjective since $\overline{f}((0,1) \otimes c) = c$ for all $c \in \mathbb{Q}$. Now consider $d = \sum n_i(a_i,b_i) \otimes c_i$ in $\ker(\overline{f})$. So $\overline{f}(d) = \sum n_ib_ic_i = 0$. Now $(a,b) \otimes c = (a,b)4 \otimes \frac{c}{4} = (0,4b) \otimes \frac{c}{4} = (0,1)4b \otimes \frac{c}{4} = (0,1) \otimes bc$. Hence $d = \sum n_i(0,1) \otimes b_ic_i = (0,1) \otimes \sum n_ib_ic_i = (0,1) \otimes 0 = 0$.

Tensor products of vector spaces. If V is a vector space over k with basis $e_1, \dots, e_n$ and W is a vector space over k with basis $f_1, \dots, f_m$, then $V \otimes_k W$ is a vector space with basis $\{e_i \otimes f_j\}$ (so dimension is nm)

To prove this, let U be a vector space with basis $\{g_{ij} : 1 \le i \le n, 1 \le j \le m\}$. Let $h : V \times W \to U$ be given by $(\sum a_ie_i, \sum b_jf_j) \mapsto \sum a_ib_jg_{ij}$. Check: h is "middle-linear". So by the proposition there exists a unique $\overline{h} : V \otimes_k W \to U$. The k-module homomorphism $\overline{h}$ is surjective since $\overline{h}(e_i \otimes f_j) = g_{ij}$. Note that if $a = \sum a_ie_i$ and $b = \sum b_jf_j$, then $a \otimes b = (\sum a_ie_i) \otimes (\sum b_jf_j) = \sum a_ib_j(e_i \otimes f_j)$. So if $\overline{h}(\sum n_{ij}e_i \otimes f_j) = 0$, then $\sum n_{ij}g_{ij} = 0$ so $n_{ij} = 0$ for all i,j, hence $\sum n_{ij}(e_i \otimes f_j) = 0$ so $\overline{h}$ is injective.

Consider $\mathbb{R} \otimes_{\mathbb{Q}} V$. Since $\mathbb{R}$ is a $\mathbb{R} - \mathbb{Q}$ bimodule, this is a left $\mathbb{R}$-module, so a vector space.

Exercise. If $\{e_i\}$ is a basis for V, then $\{1 \otimes e_i\}$ is a basis for $\mathbb{R} \otimes_{\mathbb{Q}} V$ as a $\mathbb{R}$-vector space.

Lemma 4.2. *Let R be a ring with 1 and A be a unitary left R-module. Then $R \otimes_R A \cong A$ as a left R-module.*

Proof. The map $f : R \times A \to A$ defined by $(r,a) \mapsto ra$ is "middle-linear" (check!), so $\exists! \overline{f} : R \otimes_R A \to A$ with $\overline{f}(r \otimes a) = ra$. Since $r(r' \otimes a) = rr' \otimes a$. So $\overline{f}(r(r' \otimes a)) = rr'a = r\overline{f}(r' \otimes a)$, so $\overline{f}$ is an R-module homomorphism. Since $1 \otimes a \mapsto a$, $\overline{f}$ is surjective. Note that $r \otimes a = 1 \otimes ra$, so if $\overline{f}(\sum n_i(r_i \otimes_R b_i)) = 0$ then since we have

$$\begin{aligned} \sum n_i(r_i \otimes b_i) &= \sum n_i(1 \otimes r_ib_i) \\ &= \sum 1 \otimes n_ir_ib_i \\ &= 1 \otimes \sum n_ir_ib_i \end{aligned}$$

we find $\overline{f}(\sum n_i(r_i \otimes b_i)) = \sum n_ir_ib_i = 0$, so $\sum n_i(r_i \otimes b_i) = 1 \otimes 0 = 0$. So $\overline{f}$ is injective. □

In general, if M is a left R-module, and $\phi : R \to S$ a ring homomorphism, then $S \otimes_R M$ is a left S-module. This is often called *extension of scalars* or sometime *base change.* If R, S are fields then $S \otimes_R M$ is a vector space with the same dimension of M.

Exercise. $K \subsetneq L$ fields, $L \otimes_K K[x_1, \dots, x_n] \cong L[x_1, \dots, x_n]$ (as vector spaces)

4.1 Functoriality

Suppose $\phi : M_R \to N_R$ and $\psi :_R M' \to_R N'$ are R-module homomorphisms. We will now construct $\phi \otimes \psi : M \otimes_R M' \to N \otimes_R N'$ as follows: The map $f : M \times M' \to N \otimes_R N'$ given by $(m,m') \mapsto \phi(m) \otimes \psi(m')$ is "middle-linear". Check this yourself but we can see that

$$\begin{aligned} (m_1 + m_1, m') \mapsto \phi(m_1 + m_2) \otimes \psi(m') &= (\phi(m_1) + \phi(m_2)) \otimes \psi(m') \\ &= \phi(m_1) \otimes \psi(m') + \phi(m_2) \otimes \psi(m') \\ &= f(m_1, m') + f(m_2, m') \end{aligned}$$

This gives an induced map $\overline{f} = \phi \otimes \psi : M \otimes_R M' \to N \otimes_R N'$ defined by $\phi \otimes \psi(m \otimes m') = \phi(m) \otimes \psi(m')$

If M, N are $S - R$ bimodules and ϕ is a bimodule homomorphism then $\phi \otimes \psi$ is an S-module homomorphism.

Then, given a right R-module A, we get a functor $A \otimes - :_R$Mod→Groups, it act on objects by $B \mapsto A \otimes_R B$ and on morphisms it acts by $(f : B \to C) \mapsto (1 \otimes f : A \otimes B \to A \otimes C)$. Similarly, a left R-module B gives a functor $- \otimes_R B$:Mod$_R$ →Groups.

If A is an $S - R$ bimodule, we replace Groups by $_S$Mod.

Theorem 4.3. *Let R, S be rings, let A be a right R-module, B an $R - S$ bimodule, and C a right S-module. Then* $\hom_S(A \otimes_R B, C) \cong \hom_R(A, \hom_S(B,C))$.

Note.

- Write F for the functor $-\otimes B$ and G for the functor $\hom(B,-)$. Then the theorem says $\hom_S(F(A),C) = \hom_R(A, G(C))$. When we have such a situation for a pair of functors F is called *left adjoint* to G and G is *right adjoint* to F
- If B is an $R-S$ bimodule and C is a right S module, then $\hom_S(B,C)$ is a right R-module, under the map $\psi r \in \hom_S(B,C)$ is given by $(\psi r)(b) = \psi(rb)$. Check: $(\psi r)s = \psi(rs)$ since $((\psi r)s)(b) = (\psi r)(sb) = \psi(rsb) = \psi(rs)(b)$.
- $\hom_S(B,C)$ is an abelian group $(\phi+\psi)(b) = \phi(b)+\psi(b)$. Identity: $\phi(b) = 0 \forall b \in B$.

Example. $R = S = C = K$ then $(A \otimes B)^{\mathrm{op}} \cong \hom(A, B^{\mathrm{op}})$

of Theorem 4.3. Given $\phi : A \otimes B \to C$, define $\Psi(\phi) = \psi : A \to \hom_S(B,C)$ by $\psi(a)(b) = \phi(a \otimes b)$. We check:

1. For each $a, \psi(a) \in \hom_S(B,C)$,

$$\begin{aligned}\psi(a)(b+b') &= \phi(a \otimes (b+b')) \\ &= \phi(a \otimes b + a \otimes b') \\ &= \phi(a \otimes b) + \phi(a \otimes b') \\ &= \psi(a)(b) + \psi(a)(b')\end{aligned}$$

$$\begin{aligned}\psi(a)(bs) &= \phi(a \otimes bs) \\ &= \phi((a \otimes b)s) \\ &= \phi(a \otimes b)s \text{ since } \phi \text{ is an } S\text{-module homomorphism} \\ &= \psi(a)(b)s\end{aligned}$$

2. ψ is an R-module homomorphism:

$$\begin{aligned}\psi(a+a')(b) &= \phi((a+a') \otimes b) \\ &= \phi(a \otimes b + a' \otimes b) \\ &= \phi(a \otimes b) + \phi(a' \otimes b) \\ &= \psi(a)(b) + \psi(a')(b)\,\forall b\end{aligned}$$

So $\psi(a+a') = \psi(a) + \psi(a') \in \hom_S(B,C)$

$$\begin{aligned}\psi(ar)(b) &= \phi(ar \otimes b) \\ &= \psi(a)(rb) \\ &= (\psi(a)r)(b)\end{aligned}$$

So $\psi(ar) = \psi(a)r$.

3. Ψ is a group homomorphism

$$\begin{aligned}\Psi(\phi+\phi')(a)(b) &= (\phi+\phi')(a \otimes b) \\ &= \phi(a \otimes b) + \phi'(a \otimes b) \\ &= \Psi(\phi)(a)(b) + \Psi(\phi')(a)(b)\end{aligned}$$

This is true for all a, b so $\Psi(\phi+\phi') = \Psi(\phi) + \Psi(\phi')$. Hence Ψ is a group homomorphism.

For the inverse, given an R-module homomorphism $\psi : A \to \hom_S(B,C)$ define the function $f : A \times B \to C$ by $f(a,b) = \psi(a)(b)$. This is "middle linear" (Check!). So f defines $\phi : A \otimes_R B \to C$ with $\phi(a \otimes b) = \psi(a)(b)$. This gives an inverse to Ψ. □

Example. Of Adjoints. Let F :Sets→Groups defined by $X \mapsto F(X)$ (the free group) and G :Groups→Sets the forgetful functor. Then $\hom_{\mathrm{Groups}}(FX, H) \cong \hom_{\mathrm{Sets}}(X, GH)$.

The point of all this is: if F is a left adjoint functor, then F preserves coproduct.

Example. $-\otimes B$ preserves direct sums of modules. $(A\oplus B)\otimes C\cong(A\otimes C)\oplus(B\otimes C)$.

Proposition 4.4. *Let A be a right R-module, B an $R-S$ bimodule and C a left S-module. Then $(A\otimes_R B)\otimes_S C\cong A\otimes_R(B\otimes_S C)$.*

Proof. Sketch 1 Fix C, define $A\otimes B\to A\otimes(B\otimes C)$ and define $a\otimes b\mapsto a\otimes(b\otimes c)$. This means that the map $(A\otimes B)\times C\to A\otimes(B\otimes C)$ given by $(a\otimes b,c)=a\otimes(b\otimes c)$ is well define and "middle linear". Then do the same thing for the other direction and we have an isomorphism.

Sketch 2 We construct $A\otimes_R B\otimes C$ by $F(A\times B\times C)/R$ where R is a set of relations. (For example $(a+a',b,c)=(a,b,c)+(a',b,c)$ or $(ar,b,c)=(a,rb,c)$ or $(a,bs,c)=(a,b,sc)$ etc.) Then use universal properties of categories.

$\square$

Definition 4.5. Let R be a commutative ring with identity. An *R-algebra* is a ring A with identity and a ring homomorphism $f:R\to A$ mapping 1_R to 1_A such that $f(R)$ is in the centre of A ($f(r)a=af(r)\,\forall r\in R,a\in A$). This makes A a left and right R -module.

Example. $R=k$ a field, $A=k[x_1,\ldots,x_n]$
$K\subseteq L$ fields, $R=K,A=L$
$R=K$, $A=M_n(K)$

Definition. An R-algebra *morphism* is a ring homomorphism $\phi:A\to B$ with $\phi(1_A)=1_B$ that is also an R-module homomorphism. So $\phi(ra)=r\phi(a)$.

Proposition 4.6. *Let R be a commutative ring with 1, and let A,B be R-algebras. Then $A\otimes_R B$ is an R-algebra with multiplication induced from $(a\otimes b)(a'\otimes b')=aa'\otimes bb'$.*

Proof. Once we have shown that the multiplication is well-defined, then $1\otimes 1$ is the identity and we have $f:R\to A\otimes B$ given by $f(r)=r\otimes 1=1\otimes r$. This satisfies $(r\otimes 1)(a\otimes b)=ra\otimes b=ar\otimes b=(a\otimes b)(r\otimes 1)$.

To show that the multiplication is well-defined and distributive we can construct a homomorphism $A\otimes B\otimes A\otimes B\to A\otimes B$ by $a\otimes b\otimes a'\otimes b'\mapsto aa'\otimes bb'$. We construct this map in stages: fix a',b' and construct $\phi_{a',b'}:A\otimes B\to A\otimes B$. Use $\phi_{a',b'}$to construct $\psi_b:A\otimes B\otimes A\to A\otimes B$ and thus the above map. This homomorphism is induced by a "middle linear" map $f:A\otimes B\times A\otimes B\to A\otimes B$ defined by $(a\otimes b,a'\otimes b')\mapsto(aa',bb')$ which is our multiplication. The "middle-linearity" shows distributivity. $\square$

4.2 Tensor Algebras

Let R be a commutative ring with 1 and let M be an R-module

Definition 4.7. For each $k\geq 1$, set $T^k(M)=\underbrace{M\otimes_R M\otimes_R\cdots\otimes_R M}_{k}$. So $T^0(M)=R$. Define $T(M)=R\oplus M\oplus(M\otimes M)\oplus\cdots=\bigoplus_{k=0}^{\infty}T^k(M)$. By construction this is a left and right R-module.

Theorem 4.8. *$T(M)$ is an R-algebra containing M defined by $(m_1\otimes\cdots\otimes m_i)(m_1'\otimes\cdots\otimes m_j')=m_1\otimes\cdots\otimes m_i\otimes m_1'\otimes\cdots\otimes m_j'$ and extend via distributivity. For this multiplication, $T^i(M)T^j(M)\subseteq T^{i+j}(M)$. If A is any R-algebra and $\phi:M\to A$ is a R-module homomorphism, then there exists a unique R-algebra homomorphism $\Phi:T(M)\to A$ such that $\Phi|_M=\phi$.*

Proof. The map $T^i(M)\times T^j(M)\to T^{i+j}(M)$ defined by $(m_1\otimes\cdots\otimes m_i,m_1'\otimes\cdots\otimes m_j')\mapsto(m_1\otimes\cdots\otimes m_i\otimes m_1'\otimes\cdots\otimes m_j')$ is "middle-linear" (check that this is well-defined.) So multiplication is defined and distributive. Suppose A is an R-algebra and $\phi:M\to A$ is an R-module homomorphism. Then $M\times M\to A$ defined by $(m_1,m_2)\mapsto\phi(m_1)\phi(m_2)$ is middle linear. So it defines an R-module homomorphism $M\otimes M\to A$. (Exercise: check actually we get $T^k(M)\to A$). We thus get a R-module homomorphism $\Phi:T(M)\to A$ with $\Phi|_M=\phi$. This respect multiplication, so is a ring homomorphism. Now $\Phi(1)=1$ by construction, so we have a R-algebra homomorphism. Since $\Phi(m)=\phi(m)$ for all $m\in M$, if $\Psi:T(M)\to A$ were another such R-algebra homomorphism, $\Psi(m_1\otimes\cdots\otimes m_i)=\Phi\Psi(m_1)\ldots\Psi(m_i)=\phi(m_1)\ldots\phi(m_i)=\Phi(m_1\otimes\cdots\otimes m_i)$, so $\Psi=\Phi$. $\square$

Example. $R = K$ a field, $M = V$ a d dimensional vector space with basis $e_1, \ldots, e_d$. $T^j(M)$ is a vector space with basis $e_{i_1} \otimes \cdots \otimes e_{i_j}$ and hence has dimension d^j. Multiplication is concatenation, so $T(M)$ consists of "non-commutative polynomials" in the variables $e_1, \ldots, e_d$. This is either called the "non-commutative polynomial algebra" or "free associative algebra".

$R = \mathbb{Z}$ and $M = \mathbb{Z}/6\mathbb{Z}$. Now $T^j(M) \cong \mathbb{Z}/6\mathbb{Z}$, so $T(M) \cong \mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \ldots \cong \mathbb{Z}[x]/\langle 6x \rangle$.

We work out$T(\mathbb{Q}/\mathbb{Z})$. Now $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$, to see this $\frac{a}{b} \otimes \frac{c}{d} = \frac{a}{b} \otimes \frac{b}{b}\frac{c}{d} = \left(\frac{a}{b}\right) b \otimes \frac{1}{b}\frac{c}{d} = a \otimes \frac{c}{bd} = 0 \otimes \frac{c}{bd} = 0$. So $T(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

Definition 4.9. A ring S is ($\mathbb{N}$)-*graded* if $S \cong S_0 \oplus S_1 \oplus \cdots = \oplus_{k \geq 0} S_k$ (as groups) with $S_j S_i \subseteq S_{i+j}$ and $S_i S_j \subseteq S_{i+j}$ $\forall i, j \geq 0$. The elements of S_i are called *homogeneous of degree i*. A homomorphism $\phi : S \to T$ of graded rings is *graded* if $\phi(S_k) \subseteq T_k$ for all k.

Example. $S = k[x_1, \ldots, x_n]$ or $S = T^k(M)$

Note. $S_0 S_0 \subseteq S_0$, so S_0 is a subring. Also $S_0 S_j \subseteq S_j$, so each S_j is an S_0-module. If S has an identity 1, it lives in S_0. (if not $1 = e_k + e$, $e \in \oplus_{j=0}^{k+1} S_j$, for $s \in S_1, s = 1 \cdot s = (e_k + e)s = e_k s + es \to e_k s = 0$). If S_0 is in the centre of S, then S is an S_0-algebra.

4.3 Symmetric and Exterior Algebras

Definition 4.10. The *symmetric algebra* of an R-module M is $S(M) = T(M)/C(M)$ where $C(M) = \langle m_1 \otimes m_2 - m_2 \otimes m_1 : m_1, m_2 \in M \rangle$ (two-sided ideal generated by).

Since $T(M)$ is generated as an R-algebra by T and M, and the images of $m_1 \otimes m_2$ and $m_2 \otimes m_1$ agrees in $S(M)$, we have $S(M)$ is a commutative ring. (Exercise: think about universal properties)

Example. V is a d-dimensional vector space over k, spanned by $e_1, \ldots, e_d$. Then $S(V) \cong k[x_1, \ldots, x_n]$.

Definition 4.11. The *exterior algebra* of an R-module M is the R-algebra $\wedge(M) = T(M)/A(M)$ where $A(M) = \langle m \otimes m : m \in M \rangle$. The image of $m_1 \otimes \cdots \otimes m_j$ in $\wedge M$ is written $m_1 \wedge m_2 \wedge \cdots \wedge m_j$. Multiplication is called *exterior* or *wedge product.*

Example. $M = V$ a d-dimensional vector space over k (of characteristic not 2), spanned by $e_1, \ldots, e_d$. Then $\wedge M = T(M)/A(M) = \{\text{non-commutative polynomials}\}/\langle l^2 \rangle$ where $l = \sum a_i e_i$. We see that this forces $x_i x_j = -x_j x_i$ (consider $(x_i + x_j)^2$). So in this case $\wedge V = k\langle x_1, \ldots, x_j \rangle / \langle x_i x_j + x_j x_i \rangle$. In characteristic 2, we have that $x_i x_i \notin \langle x_i x_j + x_j x_i \rangle$

Write $\wedge^k M$ for the image of $T^k(M)$ in $\wedge(M)$

Exercise. This is a graded component, i.e., $\wedge(M) = \oplus \wedge^k (M)$.

If $f \in \wedge^k M, g \in \wedge^l M$ then $fg = (-1)^{kl} gf$. This is referred as "graded commutative"

4.4 Summary

What we should remember/understand

- $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$
- $L \otimes K[x_1, \ldots, x_n]$
- $V \otimes_k W$ where V, W are vector-space over k
- $\wedge^k V$ where V is a vector-space over k.

5 Homological Algebra

Definition 5.1. A sequence $\cdots \longrightarrow M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} M_3 \xrightarrow{\phi_3} M_4 \longrightarrow \cdots$ of groups/R-modules/... is a *complex* if $\phi_{i+1} \circ \phi = 0$, i.e., $\phi_i \subseteq \ker(\phi_{i+1})$.

It is *exact* if $\ker(\phi_{i+1}) = \operatorname{im}(\phi_i)\ \forall i$.

A *short exact sequence* is $0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$. This means:

1. ϕ is injective
2. $\operatorname{im}\phi = \ker\psi$
3. ψ is surjective

A *morphism of complexes*

$$\begin{tikzcd}
\cdots \arrow[r] & A_i \arrow[r, "\delta_i"] \arrow[d, "f_i"'] & A_{i+1} \arrow[r, "\delta_{i+1}"] \arrow[d, "f_{i+1}"'] & A_{i+2} \arrow[r, "\delta_{i+2}"] \arrow[d, "f_{i+2}"'] & \cdots \\
\cdots \arrow[r] & B_i \arrow[r, "\mu_i"] & B_{i+1} \arrow[r, "\mu_{i+1}"] & B_{i+2} \arrow[r, "\mu_{i+2}"] & \cdots
\end{tikzcd}$$

is a sequences of maps $f_i : A_i \to B_i$ such that the diagram

$$\begin{tikzcd}
A_i \arrow[r, "\delta_i"] \arrow[d, "f_i"'] & A_{i+1} \arrow[d, "f_{i+1}"'] \\
B_i \arrow[r, "\mu_i"] & B_{i+1}
\end{tikzcd}$$

commutes. If all the f_i are isomorphism then the complexes are *isomorphic*.

Short 5-lemma. *Let*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\psi"] \arrow[d, "\alpha"] & B \arrow[r, "\phi"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\psi'"] & B' \arrow[r, "\phi'"] & C' \arrow[r] & 0
\end{tikzcd}$$

be morphism of short exact sequences of groups.

- *If α and γ are injective so is β.*
- *If α and γ is surjective so is β*
- *If α and γ are isomorphism so is β*

Proof. Suppose that α and γ are injective, and $\beta(b) = 0$ for some $b \in B'$. Then $\phi'\beta(b) = 0 = \gamma\phi(b)$. Since γ is injective, $\phi(b) = 0$, so $b \in \ker\phi$, hence there exists $a \in A$ such that $b = \psi(a)$. So $\beta(b) = \beta\psi(a) = \psi'\alpha(a) = 0$. Since ψ' is injective, $\alpha(a) = 0$, but α is also injective, so $\alpha = 0$. So $b = \psi(a) = 0$ and thus β is injective.

Suppose α and γ are surjective and consider $b' \in B'$. Since γ is surjective, there exists $c \in C$ with $\gamma(c) = \phi'(b')$. Since ϕ is surjective, there exists $b \in B$ with $\phi(b) = 0$, so $\gamma\phi(b) = \phi'\beta(b) = \phi'(b')$. Thus $\beta(b) = b' \in \ker\phi' = \operatorname{im}\psi'$. So there exists $a' \in A'$ with $\psi'(a') = \beta(b) - b'$. Since α is surjective, there exists $a \in A$ such that $\alpha(a) = a'$, so $\psi'\alpha(a) = \beta(b) - b'$. Thus $\beta\psi(a) = \beta(b) - b'$, so $b' = \beta(b - \psi(a)) \in \operatorname{im}\beta$. $\square$

Question: Given A, C what can you say about B with $0 \to A \to B \to C \to 0$ exact? One obvious answer is $0 \to A \overset{a \mapsto (a,0)}{\to} A \oplus C \underset{(a,c) \mapsto c}{\to} C \to 0$ is always exact.

Definition 5.2. Let R be a ring and let $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ be a short exact sequence of R-modules. The sequence is said to *split* (or *be split*) if there exists an R-submodule $D \subseteq B$ such that $B = D + \psi(A)$ with $D \cap \psi(A) = \{0\}$ (i.e., $B \cong D \oplus \psi(A)$). "There exists R-module complement of $\psi(A)$ in B"

Equivalently
$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\cong"] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & A \arrow[r] & A \oplus C \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$
is an isomorphism of complexes.

Lemma 5.3. *The short exact sequence* $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ *splits if and only if there exists* $\mu : C \to B$ *(called a* section*) such that* $\phi \circ \mu = \mathrm{id}_C$*, if and only if there exists* $\lambda : B \to A$ *such that* $\lambda \circ \psi = \mathrm{id}_A$

Note. If there exists an R-module complement D to $\psi(A)$ in B, then $D \cong B/\psi(A) \cong C$

Proof of Note. Consider $\phi : B \to C$. Note that $\phi|_D$ is injective, since $D \cap \psi(A) = \{0\}$ (as $\psi(A) = \ker \phi$). Since ϕ is surjective, for any $c \in C$, there exists $b \in B$ with $\phi(b) = c$. Write $b = d + \psi(a)$ for some $d \in D, a \in A$. But then $\phi(b) = \phi(d + \psi(a)) = \phi(d) + \phi(\psi(a)) = \phi(d)$, so $\phi|_D$ is surjective. $\square$

Proof of Lemma. If the sequence splits, there exists an R-module complement D for $\phi(A)$. By above, $D \cong C$, so let $\mu : C \to D$ be the isomorphism ($\mu = \phi^{-1}$). By construction $\phi(\mu(c)) = c$ so $\phi \circ \mu = \mathrm{id}_c$.

Conversely, if there exists $\mu : C \to B$ such that $\phi \circ \mu = \mathrm{id}_C$, let $D = \mu(C)$. We need to show that D is an R-module complement for $\psi(A)$. Let $b \in D \cap \psi(A)$. Then $b = \mu(c)$, so $\phi(B) = \phi(\mu(c)) = c$, but since $b = \psi(a)$ for some a, we have $\phi(b) = \phi(\psi(a)) = 0$, so $c = 0$ and thus $b = \mu(0) = 0$. Given $b \in B$, let $d = \mu(\phi(b))$. Then $\phi(b - d) = \phi(b - \mu\phi(b)) = \phi(b) - \phi\mu\phi(b) = \phi(b) - \phi(b) = 0$, so $b - d \in \ker \phi = \operatorname{im} \psi$. So there exists $a \in A$ such that $b = d + \phi(a)$, so $B = D + \psi(A)$ $\square$

Example. Given A and letting $C = \mathbb{Z}$, what are the options for B with $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$? In this case, $B \cong A \oplus \mathbb{Z}$, since the map $\mu : C \cong \mathbb{Z} \to B$, given by $\mu : 1 \mapsto b$ where b is a fixed choice of $b \in B$ with $\phi(b) = 1$, is a splitting. As $\phi \circ \mu(n) = \phi(nb) = n\phi(b) = n \cdot 1 = n$.

Recall that $\hom_R(D, -)$ is a functor, $f : A \to B$,$f : \hom_R(D, A) \to \hom_R(D, B)$ defined by $\phi \mapsto f \circ \phi$.

Given $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$, we can apply $\hom_R(D, -)$ to it:

$$0 \longrightarrow \hom_R(D, A) \xrightarrow{\psi} \hom_R(D, B) \xrightarrow{\phi} \hom_R(D, C) \longrightarrow 0$$

. WARNING: no claims this is a complex yet.

Claim: $0 \to A \xrightarrow{\phi} B$ is exact, then $0 \to \hom_R(D, A) \xrightarrow{\phi} \hom_R(D, B)$ is exact.

Proof. Consider $f \in \hom_R(D, A)$. If $f \neq 0$, then there exists $d \in D$ with $f(d) = a \neq 0$. Then $\phi(f)(d) = \phi(f(d)) = \phi(a) \neq 0$ since ϕ is injective. So $\phi(f)|neq0$, so $\hom_R(D, A) \xrightarrow{\phi} \hom_R(D, B)$ is injective. $\square$

Claim: If $0 \to A \xrightarrow{\psi} B \xrightarrow{\phi} C$ is exact then $\hom_R(D, A) \xrightarrow{\psi} \hom_R(D, B) \xrightarrow{\phi} \hom_R(D, C)$ is exact

Proof. Let $f \in \hom_R(D, A)$. Then for all $d \in D$, $\phi \circ \psi(f)(d) = \phi(\psi(f(d)) = 0$, so $\phi \circ \psi : \hom_R(D, A) \to \hom_R(D, C) = 0$ (i.e., this is a complex). Now consider $f \in \hom_R(D, B)$ with $\phi(f) = 0$. Then for any $d \in D$, $\phi(f(d)) = 0$, so $f(d) \in \ker \phi$, and thus there exists $a \in A$ with $\phi(a) = f(d)$. The choice of a is forced since ψ is injective.

Define $g : D \to A$ by $g(d) = a$. We now check this is an R-module homomorphism. Then $\psi g = f$, so $f \in \operatorname{im} \psi$. Suppose $g(d) = a, g(d') = a'$, then $\psi(a) = f(d), \psi(a') = f(d')$. So $\psi(a+a') = \psi(a)+\psi(a') = f(d)+f(d') = f(d+d')$. So we must have (since ψ is injective) $g(d + d') = a + a' = g(d) + g(d')$. (Check $g(rd) = rg(d)$) $\square$

However if $0 \to A \to B \to C \to 0$ we do not necessarily have $\hom_R(D, B) \to \hom_R(D, C) \to 0$ is exact.

Example. $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$, and $D = \mathbb{Z}/2\mathbb{Z}$.

Definition 5.4. We say that $\hom_R(D, -)$ is a *left exact functor.*

If F is a covariant functor, F : R-module $\to$ R-module, then F is *left exact* if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ implies $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C)$.

It is *right exact* if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ implies $F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$

Hence it is *exact* if $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ implies $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$

Question: For which D is $\hom_R(D, -)$ exact? Let $D = R$ (a ring with identity) If $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact then $0 \longrightarrow \hom_R(R, A) \longrightarrow \hom_R(R, B) \longrightarrow \hom(R, C) \longrightarrow 0$ is exact because $\hom_R(R, A) \cong A$ by $\phi \mapsto \phi(1)$ and

$$\begin{tikzcd}
f(1) & A \arrow[r, "\psi"] & B & \psi f(1) \\
f \arrow[u, mapsto] & \hom_R(R, A) \arrow[u] \arrow[r] & \hom_R(R, A) \arrow[u] & \psi f \arrow[u, mapsto] \\
 & f \arrow[r, mapsto] & \psi f &
\end{tikzcd}$$

commutes.

Definition 5.5. An R-module P is projective if for any surjection $\phi : M \to N$ of R-modules and an R-module map $f : P \to N$ such that there exists $g : P \to M$ such that $f = \phi \circ g$

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\
M \arrow[r, two heads, "\phi"] & N \arrow[r] & 0
\end{tikzcd}$$

Example. $P = R^n$ for some n

Proposition 5.6. *Let P be an R-module. The following are equivalent:*

1. *P is projective*

2. *For all short exact sequence $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ we have $0 \longrightarrow \hom_R(P, A) \longrightarrow \hom_R(P, B) \longrightarrow \hom_R(P, C) \longrightarrow 0$ is exact. (That is $\hom_R(P, -)$ is an exact functor)*

3. *There exist an R-module Q and set S such that $P \oplus Q \cong \oplus_S R$. "$P$ is a direct summand of a free module"*

Note. If $R = \mathbb{Z}, R = k[x_1, \ldots, x_n]$ then all projective modules are free. (The second is Serre's conjecture and proven by Quillen-Suslin)

Proof. $1 \Rightarrow 2$ Let $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ be a short exact sequence. Then we know $0 \longrightarrow \hom_R(P, A) \longrightarrow \hom_R(P, B) \longrightarrow \hom_R(P, C)$ is exact. Now given $f \in \hom_R(P, C)$ we have

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\
B \arrow[r, two heads, "\phi"] & C \arrow[r] & 0
\end{tikzcd}$$

so there exists a unique $g : P \to B$ such that $f = \phi \circ g$, i.e., $f = \phi(g)$. Thus $\phi : \hom_R(P, B) \to \hom_R(P, C)$ is surjective.

$2 \Rightarrow 3$ Suppose $\hom_R(P, -)$ is exact. Write $P = \oplus_{s \in S} R/K$ as a quotient of a free module. Then $0 \to K \to \oplus R \xrightarrow{\pi} P \to 0$ is exact. Since $\hom_R(P, \oplus R) \to \hom_R(P, P)$ is surjective, there exists $\mu : P \to \oplus R$ such that $\pi(\mu) = \mathrm{id} : P \to P$, i.e., for all $p \in P$ we have $\pi \circ \mu(p) = p$. Thus $\oplus R \cong P \oplus K$.

$3 \Rightarrow 1$ Suppose $P \oplus Q = F$ (where F is a free R-module, i.e., $F \cong \oplus_{s \in S} R$, S a set and let $i : S \to F$) and

$$\begin{tikzcd}
 & P \arrow[d, "f"] & \\
M \arrow[r, two heads, "\phi"] & N \arrow[r] & 0
\end{tikzcd}$$

Let $\pi : F \to P$ for the projection map. Then $f \circ \pi \in \hom(F, N)$. For each $s \in S$, let n_s be $f(\pi(i(s)))$. Choose $m_s \in M$ with $\phi(m_s) = n_s$. By the universal property there exists a unique $g : F \to M$ such that $\phi \circ g = f \circ \pi$. So we have the following commutative diagram

$$\begin{tikzcd}
 & F \arrow[d, "\pi"] \arrow[ddl, "g"'] & \\
 & P \arrow[d, "f"] & \\
M \arrow[r, two heads, "\phi"] & N \arrow[r] & 0
\end{tikzcd}$$

So define $h : P \to M$ by $h(p) = g(p, 0)$. Check: This is an R-module homomorphism. Then $\phi(h(p)) = \phi(g(p, 0)) = f(\pi(p, 0)) = f(p)$. So $\phi \circ h = f$ and so P is projective.

$\square$

Question: What about other functors? For example $\hom(-, D)$ or $A \otimes -$?

Example. $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ and apply $\hom(-, \mathbb{Z}/2\mathbb{Z})$. Then applying $\hom(-, \mathbb{Z}/2\mathbb{Z})$, we get $0 \longleftarrow \mathbb{Z}/2\mathbb{Z} \longleftarrow \mathbb{Z}/2\mathbb{Z} \longleftarrow \mathbb{Z}/2\mathbb{Z} \longleftarrow 0$, but this is not exact. To see this note that we must have

$\mathbb{Z}/2\mathbb{Z} \xleftarrow{0} \mathbb{Z}/2\mathbb{Z} \xleftarrow{\text{id}} \mathbb{Z}/2\mathbb{Z} \longleftarrow 0$, showing the failure of surjectivity.

Lemma 5.7. *Let $\psi : A \to B$, $\phi : B \to C$ be R-module homomorphism. If* $0 \longrightarrow \hom(C, D) \longrightarrow \hom(B, C) \longrightarrow \hom(A, D)$ *is exact for all R-modules D, then* $A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ *is exact.*

Proof. We need to show:

1. ϕ is surjective, use $D = C/\operatorname{im}\phi$

   Set $D = C/\phi(B)$, let $\phi_1 : C \to D$ be the projection map. Then $\pi_1 \circ \phi : B \to C/\phi(B)$ is the zero map by construction. So $\phi(\pi_1) = 0 \in \hom(B, D)$. Since $\hom(C, D) \to \hom(B, D)$ is injective, $\pi_1 = 0$, so the projection $C \to C/\phi(B)$ is the zero map. So $C/\phi(B) = 0$ and thus $\phi(B) = C$ so it is surjective.

2. $\operatorname{im}\psi \subseteq \ker\phi$, use $D = C$, $\text{id} : C \to C$

   Exercise

3. $\ker(\phi) \subseteq \operatorname{im}\psi$, use $D = B/\operatorname{im}\psi$.

   Exercise

$\square$

Proposition 5.8. *Let* $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ *be an exact sequence of R-modules. Then* $D \otimes A \xrightarrow{1 \otimes \psi} D \otimes B \xrightarrow{1 \otimes \phi} D \otimes C \longrightarrow 0$ *is exact.*

Proof. Recall $\hom(F \otimes G, H) \cong \hom(F, \hom(G, H))$. Now by left exactness of $\hom(-, E)$, for any E we have $0 \longrightarrow \hom(C, E) \longrightarrow \hom(B, E) \longrightarrow \hom(A, E)$. Then for all D

$0 \longrightarrow \hom(D, \hom(C, E)) \longrightarrow \hom(D, \hom(B, E)) \longrightarrow \hom(D, \hom(A, E))$

So $0 \longrightarrow \hom(D \otimes C, E) \longrightarrow \hom(D \otimes B, E) \longrightarrow \hom(D \otimes A, E))$ is exact. So by the lemma $D \otimes A \to D \otimes B \to D \otimes C \to 0$ is exact (Check the maps are what you think they are) $\square$

Recall: $M^\bullet$: $\ldots \longrightarrow M^{i-1} \xrightarrow{\partial_i} M^i \xrightarrow{\partial_{i+1}} M^{i+1} \xrightarrow{\partial_{1+2}} M^{i+2} \longrightarrow \ldots$ is a *complex* (or *cochain complex*) if $\partial_{j+1} \circ \partial_j = 0$ for all j

Definition 5.9. Given a (cochain) complex M, the n^{th} *cohomology* group is $H^n(M) = \ker\partial_{n+1}/\operatorname{im}\partial_n$

Notation. If $M_\bullet$ $\ldots \longrightarrow M_{i+1} \xrightarrow{\partial_{i+1}} M_i \xrightarrow{\partial_i} M_{i-1} \xrightarrow{\partial_{i-1}} M_{i-2} \longrightarrow \ldots$ is a (chain) *complex*, we write $H_n(M) = \ker\partial_n/\operatorname{im}\partial_{n+1}$ and call this the n^{th} homology group.

Definition 5.10. Let A be an R-module. A *projective resolution* of A is an exact sequence $\mathscr{P}$

$$\ldots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \xrightarrow{\partial_{n-1}} \ldots \xrightarrow{\partial_1} P_0 \xrightarrow{\epsilon} A \longrightarrow 0$$

such that each P_i is a projective module.

Example. $0 \to \mathbb{Z} \overset{\times 2}{\to} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ is a projective resolution of the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$

Note. For R-module, we can actually ask that the P_i be free R-modules. These always exists for R-modules

Let F : R-modules$\to$ R-modules be a covariant right exact functor or a contravariant left exact functor. Then applying F to $P_n \to P_{n-1} \to \cdots \to P_0 \to 0$ (forget A) gives a complex $F(\mathscr{P})$. Then the n^{th} *derived functor* of F is $H^n(F(\mathscr{P}))$

Example. F is $\hom(-, D)$. Then $F(\mathscr{P})$ is, $0 \longrightarrow \hom(P_0, D) \xrightarrow{\partial_1} \hom(P_1, D) \xrightarrow{\partial_2} \hom(P_2, D)$

Definition 5.11. With the above setting $\operatorname{Ext}^n(A, D) = \ker \partial_{n+1} / \operatorname{im} \partial_n$ for $n \geq 1$. $\operatorname{Ext}^0(A, D) = \ker \partial_1$

Example. $0 \to \mathbb{Z} \overset{\times 2}{\to} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$, what is $\operatorname{Ext}^n(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$? $0 \xleftarrow{\partial_2} \mathbb{Z}/2\mathbb{Z} \xleftarrow{0=\partial_1} \mathbb{Z}/2\mathbb{Z} \xleftarrow{\text{id}} \mathbb{Z}/2\mathbb{Z} \longleftarrow 0$. So:

- $\operatorname{Ext}^0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \ker \partial_1 = \mathbb{Z}/2\mathbb{Z}$
- $\operatorname{Ext}^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \ker \partial_2 / \operatorname{im} \partial_1 = \mathbb{Z}/2\mathbb{Z}$
- $\operatorname{Ext}^n(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = 0$ for $n \geq 2$

Theorem 5.12. $\operatorname{Ext}^n(A, D)$ *does not depend on the choice of projective resolution*

Remark. $\operatorname{Ext}^1_R(C, A)$ is in bijection with the equivalence classes of B such that $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact. "Extension of C by A"

Example. $D \otimes -$. Let $\mathscr{P}$ be a projective resolution of A: $0 \longleftarrow A \xleftarrow{\epsilon} P_0 \xleftarrow{\partial_1} P_1 \xleftarrow{\partial_2} P_2 \xleftarrow{\partial_3} \ldots$. Apply $D \otimes -$ to $\mathscr{P}$ $0 \longleftarrow D \otimes P_0 \xleftarrow{1 \otimes \partial_2} D \otimes P_1 \xleftarrow{1 \otimes \partial_2} D \otimes P_2 \xleftarrow{1 \otimes \partial_3} \ldots$ d

Definition 5.13. The n^{th} derived functor of $D \otimes -$ is called $\operatorname{Tor}^R_n(D, -)$. So $\operatorname{Tor}^R_n(D, A) = \ker \partial_n / \operatorname{im} \partial_{n+1}$ and $\operatorname{Tor}^R_0(D, A) = D \otimes P_0 / \operatorname{im} \partial$

Example. $R = \mathbb{Z}$, $A = \mathbb{Z}/7\mathbb{Z}$ and $0 \longleftarrow A \longleftarrow \mathbb{Z} \xleftarrow{\times 7} \mathbb{Z} \longleftarrow 0$ and $D = \mathbb{Z}/7\mathbb{Z}$. So we get $0 \longleftarrow \mathbb{Z}/7\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \xleftarrow{\partial_1 = 0} \mathbb{Z}/7\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \longleftarrow 0$, but $\mathbb{Z}/7\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z}$. So

- $\operatorname{Tor}^{\mathbb{Z}}_0(\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}) = (\mathbb{Z}/7\mathbb{Z}) / \operatorname{im} \partial_1 = \mathbb{Z}/7\mathbb{Z}$
- $\operatorname{Tor}^{\mathbb{Z}}_1(\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}) = (\mathbb{Z}/7\mathbb{Z})/0 = \mathbb{Z}/7\mathbb{Z}$

Remark. If A is a $\mathbb{Z}$-module (abelian group) then A is torsion free if and only if $\operatorname{Tor}_1(A, B) = 0$ for every abelian group.

Definition 5.14. A *short exact sequence of complexes* $0 \longrightarrow \mathscr{A} \xrightarrow{\psi} \mathscr{B} \xrightarrow{\phi} \mathscr{C} \longrightarrow 0$ is a set oh homomorphism of complexes such that $0 \longrightarrow A_n \xrightarrow{\psi_n} B_n \xrightarrow{\phi_n} C_n \longrightarrow 0$ is exact for every n.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\dots & A_{n+1} \arrow[l] \arrow[d, "\psi_{n+1}"'] & A_n \arrow[l] \arrow[d, "\psi_n"'] & A_{n-1} \arrow[l] \arrow[d, "\psi_{n-1}"'] & \dots \arrow[l] \\
\dots & B_{n+1} \arrow[l] \arrow[d, "\phi_{n+1}"'] & B_n \arrow[l] \arrow[d, "\phi_n"'] & B_{n-1} \arrow[l] \arrow[d, "\phi_{n-1}"'] & \dots \arrow[l] \\
\dots & C_{n+1} \arrow[l] \arrow[d] & C_n \arrow[l] \arrow[d] & C_{n-1} \arrow[l] \arrow[d] & \dots \arrow[l] \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

This diagrams commutes, the rows are complexes and the columns are exacts.

Theorem 5.15 (Long exact sequence of cohomology)**.** *Let* $0 \longrightarrow \mathscr{A} \xrightarrow{\psi} \mathscr{B} \xrightarrow{\phi} \mathscr{C} \longrightarrow 0$ *be a short exact sequence of complexes. Then there is a long exact sequence*

$$0 \longrightarrow H^0(\mathscr{A}) \longrightarrow H^0(\mathscr{B}) \longrightarrow H^0(\mathscr{C}) \xrightarrow{\partial_0} H^1(\mathscr{A}) \longrightarrow H^1(\mathscr{B}) \longrightarrow H^1(\mathscr{C}) \xrightarrow{\partial_1} H^2(\mathscr{A}) \longrightarrow \dots$$

What are the maps? Given

$$\begin{tikzcd}
A_{n-1} \arrow[r, "\partial_n"] \arrow[d, "\psi_{n-1}"'] & A_n \arrow[r, "\partial_{n+1}"] \arrow[d, "\psi_n"'] & A_{n+1} \arrow[d, "\psi_{n+1}"'] \\
B_{n-1} \arrow[r, "\mu_n"'] & B_n \arrow[r, "\mu_{n+1}"'] & B_{n+1}
\end{tikzcd}$$

We want $H^n(\mathscr{A}) \to H^n(\mathscr{B})$. Let $a \in \ker \partial_{n+1}$. Then $\psi_{n+1} \circ \partial_{n+1}(a) = 0$, so $\mu_{n+1} \circ \psi_n(a) = 0$, hence $\psi_n(a) \in \ker \mu_{n+1}$. We want $\ker \partial_{n+1} / \operatorname{im} \partial_n \to \ker \mu_{n+1} / \operatorname{im} \mu_n$. It suffices to check $\psi(\operatorname{im} \partial_n) \subseteq \operatorname{im}(\mu_n)$. If $a \in A_{n-1}$ then $\psi_n \circ \partial_n(a) = \mu_n \circ \psi_{n-1}(a) \operatorname{im}(\mu_n)$. So we get a map $H^n(\mathscr{A}) \to H^n(\mathscr{B})$ and similarly $H^n(\mathscr{B}) \to H^n(\mathscr{C})$

For the other map, we use the Snake Lemma

Snake Lemma. *Let*

$$\begin{tikzcd}
 & A \arrow[r, "\psi"] \arrow[d, "f"'] & B \arrow[r, "\phi_{n+1}"] \arrow[d, "g"'] & C \arrow[r] \arrow[d, "h"'] & 0 \\
0 \arrow[r] & A' \arrow[r, "\psi'"'] & B' \arrow[r, "\phi'"'] & C' &
\end{tikzcd}$$

be a commutative diagram with exact rows. Then there is an exact sequence

$$\ker f \longrightarrow \ker g \longrightarrow \ker h \longrightarrow \overset{\partial}{\text{c}}\text{oker}\, f \cong A' / \operatorname{im} f \longrightarrow \operatorname{coker} g \longrightarrow \operatorname{coker} h$$

Proof. Define δ: $\ker h \to \operatorname{coker} f$. Let $c \in \ker h$. Then there is $b \in B$ with $\phi(b) = c$ since ϕ is surjective. By commutativity $0 = h(c) = h \circ \phi(b) = \phi' \circ g(b)$. So $g(b) \in \ker \psi'$. By exactness there exists $a' \in A'$ such that $\psi'(a') = g(b)$. Set $\partial(c) = a' + \operatorname{im} f \in \operatorname{coker} f$.

We need to show that ∂ is well defined. Given another choice $\widetilde{b}$ with $\phi(\widetilde{b}) = c$, the difference $b - \widetilde{b} \in \ker \phi = \operatorname{im} \psi$. So there exists $a \in A$ such that $\psi(a) = b - \widetilde{b}$. But then $g\psi(a)' = g(b) - g(\widetilde{b}) = \psi' f(a)$. So $g(\widetilde{b}) = \psi'(a' - f(a))$. We then would set $\partial(c) = a' - f(a) + \operatorname{im} f = a' + \operatorname{im} f$. $\square$

6 Representation Theory

Check in this chapter whether each proposition or lemma rely on the fact that rings need to have 1.

6.1 Ring Theory for Representation Theory

Recall: Let G be a group. The group algebra $R[G] = \{\sum a_g g : a_g \in R, g \in G\} = \oplus_{g\in G} R$.

Representation theory is the study of modules over $R[G]$

Definition 6.1. An R-module $M \neq \{0\}$ is *simple* if M has no proper submodules, i.e., $N \subseteq M$ then $N = M$ or $N = \{0\}$

Proposition 6.2. *Let M and M' be simple left R-modules. Then every R-module homomorphism $f : M \to M'$ is either 0 or an isomorphism.*

Proof. Suppose f is not zero. Then $\ker(f)$ is a submodule of M that is not equal to M, so it must be the 0 module, i.e., f is injective. Similarly $\operatorname{im} f$ is a submodule of M' that is not the zero module, so $\operatorname{im} f = M'$ and thus f is surjective. So f is an isomorphism. □

A ring R is simple if ${}_R R$ is a simple R-module, e.g, $R = k$ a field

Definition 6.3. A left R-module is *semi-simple* if it is the direct sum of simple modules.

Definition 6.4. A left ideal $I \subseteq R$ is *minimal* if there exists no left ideal J of R such that $0 \subsetneq J \subsetneq I$.

Example. $R = M_n(k)$. $I = \begin{pmatrix} * & \\ \vdots & 0 \\ * & \end{pmatrix}$ is a minimal left ideal.

Definition 6.5. A ring R is (left) *semisimple* if it is isomorphic as an R-module to a direct sum of minimal left ideals. (i.e. ${}_R R$ is a semisimple R-module)

Example. $M_n(K) \cong \oplus_{j=0}^n I_j$ where $I_j = \begin{pmatrix} & * & \\ 0 & \vdots & 0 \\ & * & \\ & j^{\text{th}}\text{-column} & \end{pmatrix}$

Proposition 6.6. *A left R-module M is semisimple if and only if every submodule of M is a direct summand.*

Proof. $\Rightarrow$) Suppose M is semisimple, so $M \cong \oplus_{j\in J} S_j$. For any subset $I \subseteq J$, define $S_I = \oplus_{j\in I} S_j$. Let B be a submodule of M. Then by Zorn's lemma, there is $K \subseteq J$ maximal with respect to the property that $S_K \cap B = \{0\}$. (Suppose $K_1 \subsetneq K_2 \subsetneq \dots$ with $S_{k_i} \cap B = \{0\}$. Set $K' = \cup K_i$ and consider $S_{K'}$. If $b \in S_{K'} \cap B$ then $b \in \oplus_{j\in K'} S_j$, so $b = s_{j_1} + \dots + s_{j_r}$,$s_{j_i} \in S_{j_i}$. There is K_s with $j_1, \dots, j_r \in K_s$, so $B \in S_{K_s} \cap B$ which is a contradiction)

We claim $M = B \oplus S_K$, we just need to show that $m \in M \Rightarrow m = b + s_k$ for $b \in b, s_k \in S_K$. If $j \in K$, then $S_j \subseteq B + S_K$.

If $j \notin K$, then by maximality, $(S_K + S_j) \cap B \ni b \neq 0$. So there exists $s_K \in S_K, s_j \in S_j$ such that $s_K + s_j = b$, so $s_j = b - s_K \in S_j \cap (B + S_K) \neq 0$ since $s_j \neq 0$ as $b \notin S_K$. Thus all S_j are contained in $B + S_K$, so $M \subseteq B + S_K$.

$\Leftarrow$) Suppose every submodule of M is a direct summand. We first show that every non-zero submodule B of M contains a simple summand.

Fix $b \neq 0$ with $b \in B$. By Zorn's lemma there exists a submodule C of B maximal with respect to $b \notin C$. If $C = \{0\}$, then $B = Rb$ and B must be simple (otherwise any proper non-zero submodule would not contain b).

Otherwise write $M = C \oplus C'$, then $B = C \oplus (\underbrace{C' \cap B}_{D})$. (Since $C \cap (C' \cap B) = \{0\}$ and $b \in B \Rightarrow b = c + c'$ for $c \in C, c' \in C'$, since $b, c \in B$, $c' \in B$.) We claim that the non-zero submodule D is simple. If not by the above argument we can write, $D = D' \oplus D''$ where D', D'' are non-zero submodules of D. We claim that we do not have $b \in (C \oplus D') \cap (C \oplus D'')$. If we did, we could write $b = c + d' = c' + d''$ for $c, c' \in C$ and $d' \in D', d'' \in D''$. But then $c - c' = d'' - d' \in C \cap D = \{0\}$, so $d' = d'' \in D' \cap D'' = \{0\}$, hence $c = c' = b$ contradicting $b \notin C$. But this means one of $C \oplus D'$ and $C \oplus D''$ does not contain b, contradicting the choice of C. Thus $B = C \oplus D$ contains the simple summand D.

We now show that M is semisimple. By Zorn's lemma there is a family $\{S_j : j \in I\}$ of simple submodules of M maximal with respect to the property that the submodule U that they generated is their direct sum. By hypothesis, $M = U \oplus V$. If $V = \{0\}$, M is a direct sum of simple modules, so we are done. Otherwise V has a non-zero simple summand S, $V \cong S \oplus V'$. Then $U \cap S = \{0\}$, so $\sum S_j + S = \oplus S_j \oplus S$ contradicting the maximality of U. So $V = \{0\}$ and M is the direct sum of simple submodules. $\square$

Maschke's Theorem. *If G is a finite group and k a field with $char(K) \nmid |G|$, then $k[G]$ is semisimple. (i.e. $k[G]$ is a direct sum of simple $k[G]$-modules)*

Proof. It suffices to show that every submodule (ideal) I of kG is a direct summand. We have

$$0 \longrightarrow I \underset{\lambda}{\overset{i}{\rightleftarrows}} kG \longrightarrow \text{coker} \longrightarrow 0$$

so it suffices to construct $\lambda : kG \to I$ such that $\lambda \circ i = \mathrm{id}_I$. Since both kG and I are vector space over k, there exists $V \subseteq kG$ such that $kG \cong I \oplus V$ as vector space. Let $\pi : kG \to I$ be the projection map (it is a linear map).

Define $\lambda : kG \to kG$ by $\lambda(u) = \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}u)$. Note that $\lambda(u) \in I$, since $\pi(g^{-1}u) \in I$ and $g\pi(g^{-1}u) \in I$ as I is a left ideal. Note also that if $b \in I$ then $\lambda(b) = b$. Indeed $\lambda(b) = \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}b) = \frac{1}{|G|}\sum_{g\in G} gg^{-1}b = \frac{|G|}{|G|}b = b$.

Finally we check that λ is a kG-module homomorphism. It is straightforward to check that λ is a k-linear map, since π is. Also for $h \in G$,

$$\begin{aligned}
\lambda(hu) &= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}hu) \\
&= \frac{h}{|G|}\sum_{g\in G} h^{-}g\pi(g^{-1}hu) \\
&= \frac{h}{|G|}\sum_{g'\in G} g'\pi(g'^{-1}u) \quad \text{where } g^{'} = h^{-1}g \\
&= h\lambda(u)
\end{aligned}$$

so λ is a kG-module homomorphism with $\lambda \circ i = \mathrm{id}_I$. So I is a direct summand. $\square$

Example. $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}] = \{a(0) + b(1) : a, b \in \mathbb{C}\} = \underbrace{\mathbb{C}((0) + (1))}_{=\{a(0)+a(1):a\in\mathbb{C}\}} \oplus \underbrace{\mathbb{C}((0) - (1))}_{=\{a(0)-a(1):a\in\mathbb{C}\}}$

Definition 6.7. Let G be a group. A *representation* of G is a group homomorphism, $\phi : G \to \mathrm{GL}(V)$ where V is a vector space. It is *finite dimensional* if V is a finite dimensional vector space. V is a *simple* kG-module if V has no G-invariant subspace.

Point: If V is a vector space over k, then V is a kG-module, via $g \cdot v = \phi(g) \cdot v$.

Example. Let $G = S_3$ and $\phi : S_3 \to \mathrm{GL}_3(\mathbb{C})$ send a permutation to its permutation matrix. $\phi((1,2)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $\phi((1,2,3)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. This makes $\mathbb{C}^3$ into a $\mathbb{C}[S_3]$-module. Is it simple? The answer is no because we notice that $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ is a common subspace to both matrix. So we have $\mathbb{C}^3 \cong_{\mathbb{C}[S_3]} \text{span}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \oplus V$, where V is a 2-dimensional submodule. In fact $V = \text{span}\left(\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}\right)$. In the basis $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ for V we have $(1,2) \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $(1,2,3) \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}$.

Example. $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$, $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z}]$ and let $V = \mathbb{C}((0)+(1))$ and $W = \mathbb{F}_2((0)+(1))$. Maschke's theorem tells us that $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ is a direct summand (see previous example) but nothing about $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z}]$. In fact we can not write $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z}] \cong W\oplus ?$.

Proposition 6.8. *1. Every submodule and every quotient of a semisimple module is semisimple*

2. If R is semisimple, then every left R-module M is semisimple.

Proof. 1. Let B be a submodule of M. Every submodule C of B is a submodule of M, so $M \cong C \oplus D$ for some D. Let $\pi : M \to C$ be the projection map and let $\lambda : B \to C$ be given by $\lambda = \pi|_B$. Then

$$\begin{tikzcd} 0 \arrow[r] & C \arrow[r, shift left, "i"] & B \arrow[l, shift left, "\lambda"] \arrow[r] & \text{coker} \arrow[r] & 0 \end{tikzcd}$$

so $B \cong C \oplus \text{coker}$. So every submodule of B is a direct summand so B is semisimple.

Let M/H be a quotient of M. Since M is semisimple we have $M \cong H \oplus H'$ for some submodule H'. By the first part H' is semisimple so $M/H \cong H'$ is semisimple.

2. Suppose R is semisimple. Then any free R-module is semisimple. ($R \cong \oplus M_i$ so $\oplus R \cong \oplus \oplus M_i$) But every R-module is a quotient of a free module, so every R-module is semisimple.

□

Corollary 6.9. *Let G be a finite group and k a field with char$k \nmid |G|$. Then every kG-module is a direct sum of simple kG-modules, so every representation is a direct sum of irreducible representation.*

Proposition 6.10. *Let $R \cong_R \oplus_{i\in I} M_i$ be a semisimple ring, where the M_i are simple modules and let B be a simple R-module. Then $B \cong M_i$ for some i.*

Proof. We have $0 \neq B \cong \mathrm{Hom}_R(R, B) \cong \oplus_{i\in I} \mathrm{Hom}_R(M_i, B)$. However by Schur's Lemma $\mathrm{Hom}_R(M_i, B) = 0$ unless $M_i \cong B$. □

Corollary 6.11. *Let G be a finite group and k a field with char$k \nmid |G|$. Then there are only a finite number of simple kG-modules up to isomorphism, and thus only a finite number of irreducible representation of G.*

Example. Let $G = S_3$.

- $\phi_1 : G \to \mathbb{C}^*$, $\phi_1(g) = 1$ for all g. This corresponds to the $\mathbb{C}[S_3]$ submodule $\mathbb{C}(\sum_{g\in S_3} g)$.
- $\phi_2 : G \to \mathbb{C}^*$, $\phi_2(g) = \mathrm{sgn}(g) = \begin{cases} 1 & g \text{ is even} \\ -1 & g \text{ is odd} \end{cases}$. This corresponds to the $\mathbb{C}[S_3]$ submodule $\mathbb{C}\left(\sum_{g\in S_3} \mathrm{sgn}(g)g\right)$.
- $\phi_3 : G \to \mathrm{GL}_2(\mathbb{C})$, $\phi_3((1,2)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\phi_3((1,2,3)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

  Exercise:

  a Check that this is an irreducible representation

  b Find a two dimensional submodule of $\mathbb{C}[S_3]$ that this is isomorphic to.

So $\mathbb{C}[S_3] \cong \underset{\cong\phi_1}{\mathbb{C}} \oplus \underset{\cong\phi_2}{\mathbb{C}} \oplus \underset{\cong\phi_3}{\mathbb{C}^2} \oplus \underset{\cong\phi_3}{\mathbb{C}^2}$

Question: What are the possibilities for semisimple rings?

e.g.: $k[G]$, G finite, good characteristic. $M_n(k)$. $M_n(D)$ where D is a division ring. From these we can create more for example $M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$.

Theorem 6.12 (Wedderburn-Artin)**.** *A ring R (with 1) is semisimple if and only if R is isomorphic to a direct sum/product of matrix rings over division rings. $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$. The n_i , D_i are unique up to permutation.*

Proof. We've just discuss "if"

Suppose R is semisimple, so $R \cong_R \oplus_{i\in I} M_i$. We first note that $|I| < \infty$, since $1 \in R$, $1 = m_{i_1} + \cdots + m_{i_s}$ for some $m_{i_j} \in M_{i_j}$. So $R = R1 \subseteq M_{i_1} \oplus \cdots \oplus M_{i_s} \subseteq R$, so we have equality. After reordering, we may assume that $M_i \not\cong M_j$ for $i \neq j$, $1 \leq i, j \leq r$ and for all $j < r$ there exists $i \leq r$ with $M_j \cong M_i$. Write $B_i = \oplus_{M_j \cong M_i} M_j$, so $R \cong B_1 \oplus \cdots \oplus B_r$.

We have $R^{\text{op}} \cong \text{Hom}_R(R, R)$ (as a ring) with the map $f(1) \longleftarrow\!\shortmid f$, then $f(r) = f(r \cdot 1) = rf(1)$ and $f \circ g(1) = f(g(1)) = g(1)f(1) \longleftarrow\!\shortmid f \circ g$ So $R^{\text{op}} \cong \text{Hom}_R(R, R) \cong \text{Hom}_R(\oplus_{i=1}^r B_i, \oplus_{i=1}^r B_i) \cong \oplus_{i,j=1}^r \text{Hom}_R(B_i, B_j)$. Now $\text{Hom}_R(B_i, B_j) = \text{Hom}_R(\oplus_{l=1}^{n_i} M_l, \oplus_{k=1}^{n_j} M_k) = \oplus_{l=1}^{n_i} \oplus_{k=1}^{n_j} \text{Hom}_R(M_i, M_j) = 0$ if $i \neq j$ by Schur's Lemma. Since every non-zero function in $\text{Hom}_R(M_i, M_i)$ is an isomorphism by Schur's lemma $\text{Hom}_R(M_i, M_i)$ is a division ring with multiplication being function composition. Call this D_i^{op}. Then $\text{Hom}_R(B_i, B_i) \cong \oplus_{k,l}^{n_i} D_i^{\text{op}} \underset{\text{check}}{\cong} M_{n_i}(D_i^{\text{op}})$. So $R^{\text{op}} \cong M_{n_1}(D_1^{\text{op}}) \times \cdots \times M_{n_r}(D_r^{\text{op}})$, hence $R \cong M_{n_1}(D_1^{\text{op}})^{\text{op}} \times \cdots \times M_{n_r}(D_r^{\text{op}})^{\text{op}} = M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$.

Proof omits uniqueness. □

Exercise. $M_n(D^{\text{op}})^{\text{op}} \cong M_n(D)$

Corollary 6.13 (Molien)**.** *If G is a finite group, and k is algebraically closed, with $\text{char} k \nmid |G|$, then $k[G] \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ and thus $\sum n_i^2 = |G|$.*

Example. $\mathbb{C}[\mathbb{Z}/3\mathbb{Z}] \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$. Now $3 = n_1^2 + \cdots + n_r^2$ implies $r = 3$ and $n_1 = n_2 = n_3 = 1$. So $\mathbb{C}[\mathbb{Z}/3\mathbb{Z}] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C}$.

Let us look at the irreducible representation. We always have the "trivial representation", $\phi_1 : \mathbb{Z}/3\mathbb{Z} \to \mathbb{C}^*$ defined by $\phi_1(g) = 1$ for all g.

We then have $\phi_2((0)) = 1, \phi_2((1)) = \omega$ and $\phi_2((2)) = \omega^2$ where $\omega = e^{\frac{2\pi i}{3}}$, similarly we also get $\phi_3((0)) = 1$, $\phi_3((1)) = \omega^2$ and $\phi_3((2)) = \omega$

So then $\mathbb{C}[\mathbb{Z}/3\mathbb{Z}] \cong \underbrace{\mathbb{C}((0) + (1) + (2))}_{\phi_1} \times \underbrace{\mathbb{C}((0) + \omega^2(1) + \omega(2))}_{\phi_2} \times \underbrace{\mathbb{C}((0) + \omega(1) + \omega^2(2))}_{\phi_3}$. Check that this is a ring isomorphism e.g. $((0) + (1) + (2))((0) + \omega(1) + \omega^2(2)) = 0$.

Proof of Corollary. By Maschke's theorem $k[G]$ is semisimple, so by Wedderburn-Artin theorem $k[G] \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ where $D_i \cong \text{Hom}_{KG}(M_i, M_i)^{\text{op}}$ for simple kG-module M_i. First note that $k \subseteq \text{Hom}(M_i, M_i)^{\text{op}}$, for $a \in k$, $u \in M_i$ we set $a(u) = au$. Then $a(gu) = agu = g(au)$ so this is kG-homomorphism. Consider any $f \in D_i^{\text{op}}$, since f is a kG-homomorphism it is a linear transformation, so $f(au) = af(u)$, i.e., $(af)(u) = (fa)(u)$, so f commutes with any $a \in k$. Let $k(f)$ be the smallest sub division ring of D_i^{op} that contains k and f. The division ring $k(f)$ is a finite dimensional vector space over k.

Thus $1, f, f^2, f^3, \ldots$ are linearly dependent over k, so there exists $g \in k[X]$ with $g(f) = 0$. Take g with minimal degree. But then $\{a_0 + a_1 f + \cdots + a_r f^{\deg(g)-1} : a_i \in k\}$ is closed under addition, multiplication. Also g is an irreducible polynomial, since otherwise $g = g_1 g_2$ would imply $\underbrace{g_1(f)}_{\neq 0}\underbrace{g_2(f)}_{\neq 0} = 0$ in the division ring D_i^{op}. We show that this is closed under division. Given $h = \sum a_i f^i$, the elements $1, h, h^2, h^3, \ldots$ are linearly dependant over k. So there exists $b_i \in k$ with $\sum_{i=j\geq 0}^s b_i h^i = 0$, where we may assume that $b_j = 1$, then $\frac{1}{h} = -\sum_{i=j+1}^s b_i h^{i-j-1}$ and this can be written as $\sum_{i=0}^r c_i f^i$. Then the multiplication in $k(f)$ is commutative (since k commutes with f), so $k(f)$ is a field containing k. Since f is algebraic over the algebraically closed field k, $f \in k$. □

Question: We now have (for good k) $kG \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$. What is r?

Answer: It is the number of conjugacy class of G

Recall: A *conjugacy class* of a group G is a set $C_h = \{ghg^{-1} : g \in G\}$ of all conjugates of an element of h. The *class sum* corresponding to C_h is $z_h = \sum_{g' \in C_h} g'$. The *centre* of a ring R is $Z(R) = \{a \in R : ab = ba \, \forall b \in R\}$. e.g. The centre of $M_n(k)$ is $\{\lambda I : \lambda \in k\}$

Lemma 6.14. *Let G be a finite group. Then the class sum z_h form a k-basis for $Z(k[G])$*

Proof. First consider $z_h = \sum_{g'=ghg^{-1}} g' \in k[G]$. For any $\widetilde{g} \in G$ we have

$$\widetilde{g} z_h = \sum_{g'=ghg^{-1}} \widetilde{g} g' = \sum_{g'=ghg^{-1}} (\widetilde{g} g) g (g^{-1} \widetilde{g}^{-1}) \widetilde{g} = z_h \widetilde{g}$$

since if $g_1 \neq g_2 \in C_h$ then $\widetilde{g} g_1 \widetilde{g} \neq \widetilde{g} g_2 \widetilde{g}$. Hence $z_h \in Z(K[G])$

Now suppose $z \in \sum a_g g \in Z(k[G])$. Then for all $\widetilde{g} \in G$, $\widetilde{g} z \widetilde{g}^{-1} = \sum a_g \widetilde{g} g \widetilde{g}^{-1} = \sum a_g g$, so $a_{\widetilde{g} g \widetilde{g}^{-1}} = a_g$ and thus the coefficients of z are constant on conjugacy classes. So z is a linear combination of class sums. □

Corollary 6.15. *Let G be a finite group and k a field with $k = \overline{k}$ and char$K \nmid |G|$. Then $kG \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ where $r =$ number of conjugacy class of G.*

Proof. The centre of $M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ has dimension r over k, so $r =$ number of conjugacy classes. $\square$

Definition 6.16. Let $\phi : G \to \mathrm{GL}(V)$ be a representation of G. The *character* of ϕ is $\chi_\phi : G \to k$, $\chi_\phi(g) = \operatorname{Tr}\phi(g)$. (Note $\operatorname{Tr}(A) = \sum a_{ii}$)

Warning: This is not a group homomorphism unless $\dim V = 1$.

Note. $\chi(ghg^{-1}) = \operatorname{Tr}\phi(ghg^{-1}) = \operatorname{Tr}(\phi(g)\phi(h)\phi(g)^{-1}) = \operatorname{Tr}(\phi(h)\phi(g)\phi(g)^{-1}) = \operatorname{Tr}\phi(h) = \chi_\phi(h)$, so characters are constant on conjugacy classes.

Definition 6.17. The *character table* of a finite group G is the $r \times r$ table (where r is the number of conjugacy classes) with columns indexed by conjugacy classes and rows indexed by irreducible representation recording the character.

Example. $G = S_3$

	(1)	$(1,2),(1,3),(2,3)$	$(1,2,3),(1,3,2)$
ϕ_1	1	1	1
ϕ_2	1	-1	1
ϕ_3	2	0	-1

$G = \mathbb{Z}/3\mathbb{Z}$

	(0)	(1)	(2)
1	1	1	1
ω	1	ω	ω^2
ω^2	1	ω^2	ω

7 Galois Theory

Definition 7.1. A *field extension* L of a field K is a field L containing K. We'll write L/K or $L : K$. Given a subset X of L the intersection of all subfields of L containing K and X is denoted $K(X)$.

Example. $K = \mathbb{Q}, L = \mathbb{R}$ and $X = \{\sqrt{2}\}$ then $K(\sqrt{2}) = \{a + b\sqrt{2} : a \in \mathbb{Q}\}$.
$X = \pi$, $K(\pi) =$ set of all rational functions of π

Definition 7.2. An extension field L/K is *simple* if $L = K(\alpha)$ for some $\alpha \in L$

Example. $L = \mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$. The inclusion one way is clear. For the other way notice that $(i + \sqrt{5})^2 = 4 + 2\sqrt{5}i \in L \Rightarrow \sqrt{5}i \in L$. Also $-\sqrt{5} + 5i \in L \Rightarrow 6i \in L$ so $i \in L$.

Definition 7.3. An element $\alpha \in L$ is *algebraic* over K if there exists a monic polynomial $g \in K[x]$ with $g(\alpha) = 0$. The g of lowest degree is called the *minimal polynomial.* If α is not algebraic, it is said to be *transcendental.*

Example. $\overline{\mathbb{Q}}$ = the algebraic closure of $\mathbb{Q}$ = the set of all algebraic number over $\mathbb{Q}$. This is countable. (So transcendental elements of $\mathbb{C}$ exists)

Definition 7.4. An extension L/K is algebraic if every element of L is algebraic.

In general if α is algebraic over $\mathbb{Q}$ with a minimal polynomial f of degree d and β is algebraic over $\mathbb{Q}$ with a minimal polynomial g of degree e, what can you say about $\alpha + \beta$?

Definition 7.5. The *degree* of L/K written $[L : K]$ is the dimension of L as a vector space over K.

Note. If $L = K(\alpha)$ for α algebraic with minimal polynomial g then $[L : K] = \deg g$ since $\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg g - 1}\}$ is a basis. If α is transcendental then $L \cong K(t)$ and $[L : K] = \infty$ (define $\phi : K(t) \to K(\alpha), t \mapsto \alpha$)

The Tower Law. *Let K, L, M be fields with $K \subseteq L \subseteq M$. Then* $[M : K] = [M : L][L : K]$

Proof. Let $\{x_\alpha : \alpha \in I\}$ be a basis for L/K and let $\{y_\beta : \beta : J\}$ be a basis for M/L. Define $z_{\alpha\beta} = x_\alpha y_\beta \in M$. We claim that $\{z_{\alpha\beta}\}$ is a basis for M/K.

We show that they are linearly independent. If $\sum_{\alpha,\beta} a_{\alpha\beta} z_{\alpha\beta} = 0$ with finitely many $a_{\alpha\beta} \in K$ non-zero. Then $\sum_\beta (\sum_\alpha a_{\alpha\beta} x_\alpha) y_\beta = 0$, since the y_β are linearly independent over L we have $\sum_\alpha a_{\alpha\beta} x_\alpha = 0$ for all β. Since the x_α are linearly independent over K we have $a_{\alpha\beta} = 0$ for all α, β.

We show spanning. If $z \in M$, then $z = \sum \lambda_\beta y_\beta$ for $\lambda_\beta \in L$. For each $\lambda_\beta = \sum a_{\alpha\beta} x_\alpha$. So $x = \sum_\beta (\sum_\alpha a_{\alpha\beta} x_\alpha) y_\beta = \sum_{\alpha,\beta} a_{\alpha\beta} x_\alpha y_\beta = \sum a_{\alpha\beta} x_{\alpha\beta}$.

So $\{z_{\alpha\beta}\}$ is a basis for M over K, so $[M : K] = [M : L][L : K]$ ☐

Example. $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \times 2 = 4$. The minimal polynomial of $i + \sqrt{5}$ over $\mathbb{Q}$ is $x^4 - 8x^2 + 36$. (Note that this is not $(x^2 + 1)(x^2 - 5)$)

Definition 7.6. An *automorphism* of L is a field isomorphism $\phi : L \to L$ (so $\phi(0) = 0$ and $\phi(1) = 1$). We say ϕ *fixes* K if $\phi(a) = a$ for all $a \in K$.

Example. $\phi : \mathbb{C} \to \mathbb{C}$. $\phi(a + bi) = a - bi$ complex conjugation.
$\phi : \mathbb{Q}(\sqrt{5}, i) \to \mathbb{Q}(\sqrt{5}, i)$ defined by $\phi(a + b\sqrt{5} + ci + d\sqrt{5}i) = a - b\sqrt{5} + ci - d\sqrt{5}i$. Note ϕ fixes $\mathbb{Q}(i)$ but not $\mathbb{Q}(\sqrt{5})$.

Definition 7.7. The Galois group $\mathrm{Gal}(L/K)$ of L/K is the group of all automorphisms of L fixing K.

Example. Using the ϕ defined in the second part of the previous example, we have $\phi \in \mathrm{Gal}(\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}(i))$ but not in $\mathrm{Gal}(\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}(\sqrt{5}))$.
$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ (generated by complex conjugation) (Because $\phi(a+bi) = a + b\phi(i)$ and $\phi(i)^2 = \phi(-1) = -1$)

Note that $\mathrm{Gal}(L/K)$ is a group under function composition. $\phi : L \to L, \psi : L \to L$, $\phi(a) = \psi(a) = a$ for $a \in K$. $\phi \circ \psi : L \to L$ is an isomorphism and $\phi\psi(a) = \phi(\psi(a)) = \phi(a) = a$ for $a \in K$

Example. $\mathrm{Gal}(\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

Definition 7.8. For a subgroup H of $\mathrm{Gal}(L/K)$ we denote by L^H the set $L^H = \{\alpha \in L : \phi(\alpha) = \alpha \text{ for all } \alpha \in H\}$. This is a subfield of L called the *fixed field of H*

Example. $H = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, $\mathbb{C}^H = \mathbb{R}$.

$\mathrm{Gal}(\mathbb{Q}(\sqrt{5}, i)/\mathbb{Q}) = \langle \phi_1, \phi_2 \rangle$ where $\phi_1(i) = -i, \phi_1(\sqrt{5}) = \sqrt{5}$ and $\phi_2(i) = i, \phi_2(\sqrt{5}) = -\sqrt{5}$. Let $H_i = \langle \phi_i \rangle$. Then $\mathbb{Q}(\sqrt{5}, i)^{H_1} = \mathbb{Q}(i), \mathbb{Q}(\sqrt{5}, i)^{H_2} = \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{5}, i)^{\mathrm{Gal}} = \mathbb{Q}$. Define $H_3 = \langle \phi_3 \rangle$, where $\phi_3(i) = -i$ and $\phi_3(\sqrt{5}) = -\sqrt{5}$.

$$\begin{tikzcd}
 & \mathrm{Gal} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & H_3 \arrow[d, dash] & H_2 \arrow[dl, dash] \\
 & 1 &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{5}, i) = \mathbb{Q}(\sqrt{5}, i)^1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{5}, i)^{H_2} \arrow[dr, dash] & \mathbb{Q}(i\sqrt{5}) = \mathbb{Q}(\sqrt{5}, i)^{H_3} \arrow[d, dash] & \mathbb{Q}(i) = \mathbb{Q}(\sqrt{5}, i)^{H_1} \arrow[dl, dash] \\
 & \mathbb{Q} = \mathbb{Q}(\sqrt{5}, i)^{\mathrm{Gal}} &
\end{tikzcd}$$

Note. For any subgroup H of $\mathrm{Gal}(L/K)$ we have $K \subseteq L^H \subseteq L$ and $H \leq \mathrm{Gal}(L/L^H) \leq \mathrm{Gal}(L/K)$

Definition 7.9. A polynomial $f \in K[x]$ splits over K if $f = a \prod_{i=1}^{d}(x - b_i)$, $a, b_1, \ldots, b_d \in K$

Example. e$f = x^3 - 2$ splits over $\mathbb{C}$ Note $f = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$ where $\omega = e^{\frac{2\pi i}{3}}$. So we see that f does not split over $\mathbb{Q}(\sqrt[3]{2})$

Definition 7.10. A field L is a splitting field for a polynomial $f \in K[x]$ if $K \subseteq L$ and

1. f splits over L
2. If $K \subseteq M \subseteq L$ and splits over M then $M = L$

(Equivalently $L = K(\sigma_1, \ldots, \sigma_d)$ where $\sigma_1, \ldots, \sigma_d$ are the roots of f in L)

These always exist, and are unique up to isomorphism. The proof uses induction on $\deg f$, where we use the intermediate field $M = K[x]/(f)$.

Example. $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is a splitting field for $f = x^3 - 2$ (where $\omega = e^{\frac{2\pi i}{3}}$)

Definition 7.11. An extension L/K is *normal* if every irreducible polynomial f over K which has at least one root in L splits over L.

Example. $\mathbb{C}/\mathbb{R}$ is normal

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

Definition 7.12. An irreducible polynomial $f \in K[x]$ is *separable* over K if it has no multiple zeros in a splitting field, (i.e, the b_i are distinct). Otherwise it is *inseparable*

Example. $x^4 + x^3 + x^2 + x + 1$ is separable, its roots are ω^j, $j = 1, \ldots, 4$ where $\omega^5 = 1$

$K = \mathbb{F}_2(x)$, $f(t) = t^2 + x$ is inseparable. $K \subseteq L$ where $y \in L$ satisfies $f(y) = 0$. $f(y) = y^2 + x = 0$, $x = y^2$, so $f = t^2 + y^2 = (t + y)^2$

Proposition 7.13. *If K is a field of characteristic 0, then every irreducible polynomial is separable over K.*

If K has characteristic $p > 0$, then f is separable unless $f = g(x^p)$.

Recall: A polynomial $f \in K[x]$ has a double root if and only if f and f' (the formal derivative) have a common factor. If f had a double root and $f' \neq 0$, f and f' would have a common factor in $K[x]$ (by the Euclidean algorithm). But since $\deg(f') < \deg(f)$, this factor is not f, contradicting f being irreducible, unless $f' = 0$. We only have $f' = 0$ if $\mathrm{char} K = p$ and $f = g(x^p)$.

Definition 7.14. An algebraic extension L/K is *separable* if for $\alpha \in L$, its minimal polynomial is separable over K.

Theorem 7.15 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite separable normal field extension with $[L : K] = n$ and Gal$(L/K) = G$ then*

1. $|G| = n$

2. For $K \subseteq M \subseteq L$ we have $M = L^{\mathrm{Gal}(L/M)}$ and $H = \mathrm{Gal}(L/L^H)$, so $H \mapsto L^H$ is an order reversing bijection between the poset of subgroups of G and subfields $K \subseteq M \subseteq L$

3. If $K \subseteq M \subseteq L$ then $[L : M] = |Gal(L/M)|$ and $[M : K] = |G|/|Gal(L/M)|$

4. M/K is normal if and only if $Gal(L/M)$ is a normal subgroup of $Gal(L/K)$. In that case $Gal(M/K) \cong G/Gal(L/M)$

Corollary 7.16. *1. If L/K is finite, normal, separable then there are only finitely many fields M with $K \subseteq M \subseteq L$.*

2. If $Gal(L/K)$ is abelian, then for any $K \subseteq M \subseteq L$ we have M/K normal.

We see from this that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = S_3$ since $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal (exercise: show this directly by writing down 6 automorphism)

Galois' Application: $\mathrm{Gal}(L/K)$ simple implies no intermediate normal M/K, This in terns implies no highest degree polynomial "solved by radicals"

Proof of the Fundamental Theorem of Galois Theory (in ideas).

Lemma 7.17. *If $\phi_i : M \to L$, $i = 1, \dots, r$ are distinct inclusion of fields, then the ϕ_i are linearly independent over L, i.e., $\sum a_i \phi_i(m) = 0 \,\forall m$ then $a_i = 0 \forall i$.*

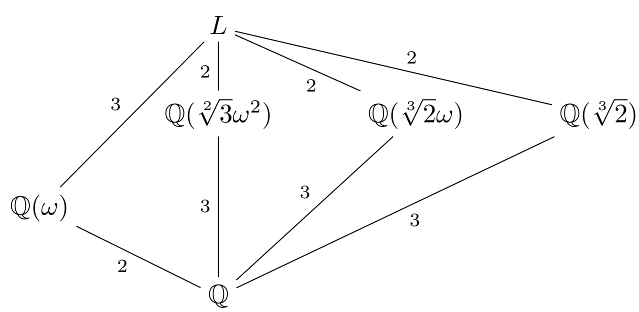
We apply this to $M = L$. For H a subgroup of $\mathrm{Gal}(L/K)$ we use the lemma to show that $[L : L^H] = |H|$. ($\{\phi \in H\}$ are linearly independent $\phi : L \to L$). So $[L^H : K] = [L : K]/|H|$. Next we use the following propositions

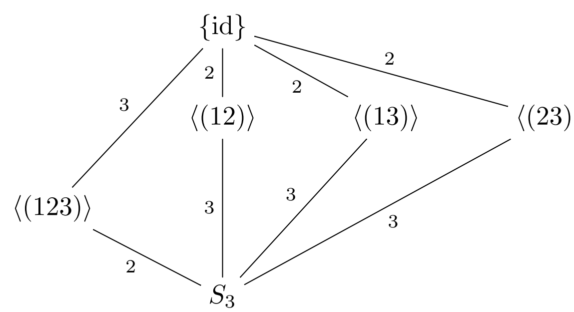
Proposition 7.18. *If L/K is normal and $K \subseteq M \subseteq L$ has M/K normal then for all $\phi \in Gal(L/K), \phi(M) = M$*

We use twice. Once for 4. and first to show that the $[L : K]$ maps $L \to N$ (where N is a bigger field) we construct by hand have image in L. Use this to show $|\mathrm{Gal}(L/K)| = [L : K]$, thus $L^{\mathrm{Gal}(L/K)} = K$, because $[L : L^{\mathrm{Gal}(L/K)}] = |G| = [L : K]$. □

Example.

- $K = \mathbb{Q}$, $L =$ splitting field of $x^3 - 2$, that is $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{\frac{2\pi i}{3}}$. Now $K \leq L$ if finite, separable (characteristic 0) and normal. What is $\mathrm{Gal}(L/K) = G$? Any elements of G permutes $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$. So $G \subseteq S_3$, but since G is of order $6 = [L : K]$, we must have $G = S_3$.





- Let $K = \mathbb{Q}$ and L be the splitting field of $x^3 - 3x - 1 = (x - \alpha)(x - \beta)(x - \gamma)$. Then $\mathbb{Q} \leq L = \mathbb{Q}(\alpha, \beta, \gamma)$. What is $\mathrm{Gal}(L/K) = ?$ So $G \subseteq S_3$. Using the fact about discriminant (see below) we have that no transposition is in G. (Since $(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = \pm 9$.) Hence we have $|G| = 3$ so $G = \mathbb{Z}/3\mathbb{Z}$.

Fact. *If L is the splitting field of a cubic then* $Gal(L/K) = \begin{cases} \mathbb{Z}/3\mathbb{Z} & \Delta(f) \text{ is a square in } \mathbb{Q} \\ S_3 & \text{otherwise} \end{cases}$

Definition 7.19. The *discriminant* of a polynomial f with roots $\alpha_1, \alpha_2, \dots, \alpha_n$ is $\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$

Fact. *You can express $\Delta(f)$ as a polynomial on the coefficients of f*

Example. If $f = x^3 - ax^2 + bx - c$, $\Delta(f) = a^2b^2 + 18abc - 27c^2 - 4a^3c - 4b^3$