

## Abstract

These notes are based on Tony Pantev’s “Algebra II” lectures at UPenn. Any mistake in what follows is my own.

## Contents

<b>1</b>	<b>Injective and flat modules</b>	<b>3</b>
1.1	Lecture 1 . . . . .	3
1.2	Lecture 2 . . . . .	5
1.3	Lecture 3 . . . . .	9
<b>2</b>	<b>Localization</b>	<b>11</b>
2.1	Lecture 4 . . . . .	11
2.2	Lecture 5 . . . . .	12
2.3	Lecture 6 . . . . .	13
2.4	Lecture 7 . . . . .	15
<b>3</b>	<b>Basic algebraic geometry</b>	<b>17</b>
3.1	Lecture 8 . . . . .	18
3.2	Lecture 9 . . . . .	20
<b>4</b>	<b>Algebraic extensions</b>	<b>23</b>
4.1	Lecture 10 . . . . .	23
4.2	Lecture 11 . . . . .	25
<b>5</b>	<b>Splitting fields</b>	<b>27</b>
5.1	Lecture 12 . . . . .	27
<b>6</b>	<b>Finite fields</b>	<b>29</b>
6.1	Lecture 13 . . . . .	29
6.2	Lecture 14 . . . . .	31
<b>7</b>	<b>Cyclotomic fields</b>	<b>32</b>
7.1	Lecture 15 . . . . .	35
<b>8</b>	<b>Galois theory</b>	<b>36</b>
8.1	Lecture 16 . . . . .	37
8.2	Lecture 17 . . . . .	39
8.3	Lecture 18 . . . . .	42

<b>9 Solvability in radicals</b>	<b>43</b>
9.1 Lecture 19 . . . . .	44
9.2 Lecture 20 . . . . .	46
9.3 Lecture 21 . . . . .	49
<b>10 Further applications of Galois theory</b>	<b>50</b>
10.1 Lecture 22 . . . . .	50
10.2 Lecture 23 . . . . .	52
<b>11 Chain complexes and chain maps</b>	<b>54</b>
11.1 Lecture 24 . . . . .	55
11.2 Lecture 25 . . . . .	57
<b>12 Additive categories</b>	<b>60</b>
12.1 Lecture 26 . . . . .	61
<b>13 Triangulated categories</b>	<b>64</b>
13.1 Lecture 27 . . . . .	64
13.2 Lecture 28 . . . . .	67
13.3 Lecture 29 . . . . .	70

# 1 Injective and flat modules

## 1.1 Lecture 1

**Proposition 1.1.1.** *An  $R$ -module  $M$  is injective if and only if we can fill any injectivity diagram of ideal type, i.e.,*

$$\begin{array}{ccccc} & & & & M \\ & & & \nearrow & \uparrow \\ 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & R \end{array}$$

where  $\mathfrak{a}$  is an ideal in  $R$ .

*Proof.*

( $\Rightarrow$ )

This is obvious.

( $\Leftarrow$ )

Let

$$\begin{array}{ccccc} & & & & M \\ & & & \nearrow \varphi & \\ 0 & \longrightarrow & X' & \longrightarrow & X \end{array}$$

be an injectivity diagram of  $R$ -modules and define

$$S = \{(A, \xi) \mid X' \subset A \subset X, \xi : A \rightarrow M, \xi|_{X'} = \varphi\}.$$

By Zorn's lemma, there is some maximal element  $(N, \psi)$  of  $S$ . Suppose, toward a contradiction, that  $X \neq N$ . Pick any  $x \in X \setminus N$ . We have the ideal

$$\mathfrak{a} := \{a \in R : ax \in N\}$$

in  $R$ . Define the  $R$ -module morphism  $\theta : \mathfrak{a} \rightarrow M$  by  $a \mapsto \psi(ax)$ . By hypothesis, we get the following commutative diagram.

$$\begin{array}{ccccc} & & & & M \\ & & & \nearrow \theta & \uparrow \tilde{\theta} \\ 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & R \end{array}$$

Define the  $R$ -submodule  $\tilde{N} = \langle N, x \rangle$ . We can write any  $z \in \tilde{N}$  as  $z = y + ax$  for some  $y \in N$  and some  $a \in R$ . Define  $\tilde{\psi} : \tilde{N} \rightarrow M$  by  $y + ax \mapsto \psi(y) + \tilde{\theta}(a)$ . To see that this is well-defined, let  $y + ax = y' + a'x$ . Then  $(y - y') = (a' - a)x$ , so that

$$\psi(y - y') = \psi((a' - a)x) = \tilde{\theta}(a' - a) = \tilde{\theta}(a') - \tilde{\theta}(a).$$

This implies that  $\tilde{\psi}$  is a well-defined homomorphism. But then  $(\tilde{N}, \tilde{\psi}) > (N, \psi)$ , a contradiction.  $\square$

*Aside.* The categorical dual  $P^{\text{op}}$  of this recognition principle for injectivity expresses a recognition principle for projectivity, namely that for any  $R$ -module  $M$ , ideal  $I \subset R$ , and homomorphism  $\varphi : M \rightarrow R/I$ , we can fill the diagram

$$\begin{array}{ccc} M & & \\ \downarrow & \searrow \varphi & \\ R & \twoheadrightarrow R/I & \longrightarrow 0 \end{array} \quad (*)$$

if and only if  $M$  is projective. This is equivalent to saying that  $M$  is projective if and only if the obvious group map  $\text{Hom}_R(M, R) \rightarrow \text{Hom}_R(M, R/I)$  is surjective. But then  $P^{\text{op}}$  is precisely an affirmative answer to what is known as “Faith’s problem on  $R$ -projectivity,” which Trlifaj (2017) proved to be undecidable in  $\text{ZFC} + \text{GCH}$ . Therefore, both  $P^{\text{op}}$  and  $\neg(P^{\text{op}})$  are consistent with  $\text{ZFC} + \text{GCH}$ .

**Corollary 1.1.2.**

1. If  $R$  is an integral domain, then any injective  $R$ -module  $M$  is divisible.
2. If  $R$  is a PID, then  $M$  is injective if and only if it is divisible.

*Proof.*

1. Given any  $a \in R$ , we want to show that the homomorphism  $\text{mult}_a : M \rightarrow M$  given by  $x \mapsto ax$  is surjective. The assumption that  $R$  is an integral domain entails that  $\text{mult}_a : R \rightarrow R$  is injective. Note that  $\mathfrak{a} := \text{mult}_a(R)$  is an ideal in  $R$ , giving the short exact sequence

$$0 \rightarrow \mathfrak{a} \rightarrow R \rightarrow R/\mathfrak{a} \rightarrow 0.$$

By assumption,  $\text{Hom}_R(-, M)$  is exact, so that the sequence

$$0 \rightarrow \text{Hom}(R/\mathfrak{a}, M) \rightarrow \text{Hom}_R(R, M) \rightarrow \text{Hom}_R(\mathfrak{a}, M) \rightarrow 0$$

is exact. Since  $R$  and  $\mathfrak{a}$  are free  $R$ -modules of rank 1, it follows that  $\text{Hom}_R(R, M) \cong M \cong \text{Hom}_R(\mathfrak{a}, M)$ . This means that the sequence

$$0 \rightarrow \text{Hom}(R/\mathfrak{a}, M) \rightarrow M \xrightarrow{\text{mult}_a} M \rightarrow 0$$

is exact. In particular  $\text{mult}_a$  is surjective.

2. ( $\Leftarrow$ ) Suppose that  $M$  is divisible and  $R$  is a PID. We want to fill the injectivity diagram

$$\begin{array}{ccccc} & & & M & \\ & & \nearrow \varphi & \uparrow \psi & \\ 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & R \end{array} .$$

where  $\mathfrak{a}$  is an ideal in  $R$ . We have that  $\mathfrak{a} = (a)$ . Therefore, the short exact sequence

$$0 \rightarrow \mathfrak{a} \rightarrow R \rightarrow R/\mathfrak{a} \rightarrow 0$$

is isomorphic to  $0 \rightarrow R \xrightarrow{\text{mult}_a} R \rightarrow R/\mathfrak{a} \rightarrow 0$ . Since  $M$  is divisible, we know that  $M \xrightarrow{\text{mult}_a} M \rightarrow 0$  is exact. Apply  $\text{Hom}_R(-, M)$  to get the sequence

$$\text{Hom}_R(R, M) \xrightarrow{(-) \circ \text{mult}_a} \text{Hom}_R(R, M) \rightarrow 0,$$

which is isomorphic to  $M \xrightarrow{\text{mult}_a} M \rightarrow 0$ . This shows that  $\text{Hom}_R(R, M) \xrightarrow{(-) \circ \text{mult}_a} \text{Hom}_R(R, M)$  is surjective. It follows that  $\varphi$  can be lifted to some  $\psi : R \rightarrow M$ .

□

## 1.2 Lecture 2

**Corollary 1.2.1.** *Any abelian group is injective if and only if it's divisible.*

**Corollary 1.2.2.** *If  $R$  is a PID and  $M$  is an injective  $R$ -module, then every quotient of  $M$  is injective.*

*Proof.* This follows from the fact that any quotient of a divisible group is divisible. □

**Example 1.2.3.**

1.  $\mathbb{Q}/\mathbb{Z}$  is injective.
2.  $S^1$  is injective.
3. Any non-trivial finitely generated abelian group  $G$  is never injective.

*Proof.* It suffices to show that  $G$  is never divisible. There exists a maximal proper subgroup  $H \leq G$ . Then  $G/H$  is a simple abelian group, so that  $G/H \cong C_p$  for some prime  $p$ . If  $G$  is divisible, then so must  $G/H$ . But  $C_p$  is not divisible, a contradiction. □

**Theorem 1.2.4 (Baer embedding).** *If  $R$  is a ring, then every module embeds into an injective module.*

**Corollary 1.2.5.** *For any  $R$ -module  $M$ , we can find an injective resolution*

$$0 \rightarrow M \rightarrow I_0 \rightarrow I_1 \rightarrow \cdots \rightarrow I_k \rightarrow \cdots$$

*Proof.* We want to invent a duality operation that will convert  $R\text{-Mod}^{\text{op}}$  to  $R^{\text{op}}\text{-Mod}$  and then use projective objects in  $R^{\text{op}}\text{-Mod}$ . If  $T$  is an abelian group, then the functor

$$\mathbf{Ab} \xrightarrow{\text{Hom}_{\mathbf{Ab}}(-, T)} \mathbf{Ab}^{\text{op}}$$

will reverse arrows. The choice of  $T$  that ends up working is precisely  $\mathbb{Q}/\mathbb{Z}$ .

**Claim.** *Let  $\text{Hom}_{\mathbf{Ab}}(-, \mathbb{Q}/\mathbb{Z}) := (-)^D$ . Note that for any abelian group  $A$ , we have a canonical homomorphism  $\epsilon_A : A \rightarrow A^{DD}$  given by  $a \mapsto ([\varphi : A \rightarrow \mathbb{Q}/\mathbb{Z}] \rightarrow \varphi(a))$ . Then  $\epsilon_A$  is injective.*

*Proof.* We need to show that if  $a \in A$  is nonzero, then we can find some homomorphism  $f : A \rightarrow \mathbb{Q}/\mathbb{Z}$  such that  $f(a) \neq 0$ .

Case 1: Suppose that  $|(a)| = n < \infty$ . Then define the homomorphism  $\varphi : (a) \rightarrow \mathbb{Q}/\mathbb{Z}$  by  $a \mapsto [\frac{1}{n}]$ . Since  $\mathbb{Q}/\mathbb{Z}$  is divisible in **Ab**, it is also injective. Thus, we may find some map  $\psi$  such that

$$\begin{array}{ccccc} & & & \mathbb{Q}/\mathbb{Z} & \\ & & \nearrow \varphi & \uparrow \psi & \\ 0 & \longrightarrow & (a) & \hookrightarrow & A \end{array}$$

commutes. This means that  $\psi(a) \neq 0$ , as required.

Case 2: If  $(a)$  has infinite order, then define  $\varphi : (a) \rightarrow \mathbb{Q}/\mathbb{Z}$  by  $a \mapsto \frac{1}{2}$  and apply a similar argument to Case 1.  $\square$

The duality functor  $(-)^D$  extends to a functor  $(-)^D : R^{\text{op}}\text{-Mod} \rightarrow R\text{-Mod}^{\text{op}}$  that is compatible with forgetting the module structure. Indeed, if  $M$  is a left module over  $R^{\text{op}}$ , then its module structure is given by a collection of maps  $\{\text{mult}_a : M \rightarrow M \mid a \in R\}$ . Note that

$$\text{mult}_a \circ \text{mult}_b = \text{mult}_{a \cdot_{R^{\text{op}}} b} = \text{mult}_{b \cdot_R a}.$$

For each  $a \in R$ , let  $\underline{\text{mult}}_a(\varphi) = \varphi \circ \text{mult}_a$ . Then the abelian group  $M^D$  has an  $R$ -module structure given by  $\underline{\text{mult}}_a : M^D \rightarrow M^D$ , which clearly satisfies

$$\underline{\text{mult}}_{ab} = \underline{\text{mult}}_a \circ \underline{\text{mult}}_b.$$

**Lemma 1.2.6.** *If  $M$  is a projective  $R^{\text{op}}$ -module, then  $M^D$  is an injective  $R$ -module.*

*Proof.* Suppose that  $M$  is a projective  $R^{\text{op}}$ -module and consider the injectivity diagram

$$\begin{array}{ccccc} & & & M^D & \\ & & \nearrow \varphi & & \\ 0 & \longrightarrow & X' & \longrightarrow & X \end{array}$$

of  $R$ -modules. We want to lift  $\varphi : X' \rightarrow M^D$  to a map  $\psi : X \rightarrow M^D$ . Apply  $(-)^D$  to get the commutative diagram

$$\begin{array}{ccccc} & & & M^{DD} & \\ & & \nwarrow \varphi^D & & \\ 0 & \longleftarrow & (X')^D & \longleftarrow & X^D \end{array}$$

where the bottom row is exact because  $\mathbb{Q}/\mathbb{Z}$  is injective.

**Exercise 1.2.7.** *Show that  $\epsilon_M : M \rightarrow M^{DD}$  is a map of  $R^{\text{op}}$ -modules.*

We now have the following projectivity diagram of  $R^{\text{op}}$ -modules.

$$\begin{array}{ccccc} M & & & & \\ & \searrow \epsilon_M \circ \varphi^D & & & \\ X^D & \longrightarrow & (X')^D & \longrightarrow & 0 \end{array}$$

By assumption, we may fill this diagram with some map  $\psi : M \rightarrow X^D$ . This induces the map  $\psi^D : X^{DD} \rightarrow M^D$ . Note that  $(\epsilon_M)^D \circ \varphi^{DD} = \psi^D \circ i^{DD}$  where  $i : X' \hookrightarrow X$ . But  $i^{DD} \upharpoonright_{X'} = i$  and  $\varphi^{DD} \upharpoonright_{X'} = \varphi$ , so that

$$\psi^D \circ i = (\epsilon_M)^D \circ \varphi = \varphi$$

on  $X'$ . It follows that

$$\begin{array}{ccccc} & & & M^D & \\ & & \nearrow \varphi & \uparrow \psi^D \circ \epsilon_X & \\ 0 & \longrightarrow & X' & \longrightarrow & X \end{array}$$

commutes. □

There is some surjection  $\bigoplus_{j \in J} R \rightarrow M^D$ . Therefore, we have a sequence of embeddings

$$M \hookrightarrow M^{DD} = \text{Hom}_{\mathbb{Z}}(M^D, \mathbb{Q}/\mathbb{Z}) \hookrightarrow \text{Hom}_{\mathbb{Z}}\left(\bigoplus_{j \in J} R, \mathbb{Q}/\mathbb{Z}\right) = \underbrace{\left(\bigoplus_{j \in J} R\right)^D}_{\text{injective by Lemma 1.2.6}}.$$

□

**Definition 1.2.8.** Given two  $R$ -modules  $M$  and  $N$ , the *additive invariants* of  $M$  and  $N$  are the abelian groups

$$\text{Ext}_R^i(M, N) := H^i(\text{Hom}_R(P^\bullet, N))$$

indexed by  $\mathbb{N}$  where  $P^\bullet$  is a chosen projective resolution of  $M$ .

**Proposition 1.2.9.**

1.  $\text{Ext}_R^i(M, N)$  is independent of the choice of projective resolution.

*Proof.* This follows from the fact that any two projective resolutions are chain homotopic. □

2.  $\text{Ext}_R^i(M, N) = H^i(\text{Hom}_R(M, I_\bullet))$  for any injective resolution  $I_\bullet$  of  $N$ .

**Lemma 1.2.10.**

1.  $\text{Ext}_R^0(M, N) = \text{Hom}_R(M, N)$
2.  $\text{Ext}_R^1(M, N) = (\text{the group of isomorphism classes of extensions of } N \text{ by } M \text{ in } R\text{-}\mathbf{Mod})$ .

*Proof.* Let

$$\dots \xrightarrow{\partial_1} P^1 \xrightarrow{\partial_0} P^0 \xrightarrow{\epsilon} M \rightarrow 0$$

be a projective resolution and let

$$(\xi) : 0 \rightarrow N \xrightarrow{f} T \xrightarrow{g} M \rightarrow 0$$

be a short exact sequence of  $R$ -modules. Note that  $\text{Hom}_R(P^k, -)$  is exact for each  $k \geq 0$ . Therefore, the sequence

$$0 \rightarrow \text{Hom}_R(P^k, N) \xrightarrow{f_k} \text{Hom}_R(P^k, T) \xrightarrow{g_k} \text{Hom}_R(P^k, M) \rightarrow 0$$

is exact where  $f_k := f \circ (-)$  and  $g_k := g \circ (-)$ . Letting  $d_i := (-) \circ \partial_i$ , we get *short exact sequences of complexes* constituting the columns of

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_R(P^0, N) & \xrightarrow{f_0} & \text{Hom}_R(P^0, T) & \xrightarrow{g_0} & \text{Hom}_R(P^0, M) \longrightarrow 0 \\ & & \downarrow d_0 & & \downarrow d_0 & & \downarrow d_0 \\ 0 & \longrightarrow & \text{Hom}_R(P^1, N) & \xrightarrow{f_1} & \text{Hom}_R(P^1, T) & \xrightarrow{g_1} & \text{Hom}_R(P^1, M) \longrightarrow 0 \\ & & \downarrow d_1 & & \downarrow d_1 & & \downarrow d_1 \\ & & \vdots & & \vdots & & \vdots \end{array}$$

By definition,  $\text{Ext}_R^i(M, N) = \overbrace{\ker d_i / \text{im } d_{i-1}}^{\text{for the first column}}$ . Since  $\text{Hom}_R(-, M)$  is left-exact and  $P^1 \xrightarrow{\partial_1} P^0 \xrightarrow{\epsilon} M$  is exact, we also have the exact sequence

$$0 \rightarrow \text{Hom}_R(M, M) \xrightarrow{(-) \circ \epsilon} \text{Hom}_R(P^0, M) \xrightarrow{d_0} \text{Hom}_R(P^1, M).$$

Let  $\psi \in \text{Hom}_R(P^0, M)$  satisfy  $d_0(\psi) = 0$ . Then  $\psi = \varphi \circ \epsilon$  for some unique map  $\varphi : M \rightarrow M$ . Since  $g_0$  is surjective, there exists  $\alpha \in \text{Hom}_R(P^0, T)$  such that  $g_0(\alpha) = \psi = \varphi \circ \epsilon$ . This implies that

$$g_1(d_0(\alpha)) = d_0(g_0(\alpha)) = d_0(\psi) = 0.$$

It follows that  $d_0(\alpha) \in \ker g_1 = \text{im } f_1$ , so that  $d_0(\alpha) = f_1(\beta)$  for some  $\beta : P^1 \rightarrow N$ . Since  $f_2(d_1(\beta)) = d_1(f_1(\beta)) = d_1(d_0(\alpha)) = 0$ , the fact that  $f_2$  is injective means that  $d_1(\beta) = 0$ . Hence  $\beta \in \ker d_1$ , and  $[\beta] \in \text{Ext}_R^1(M, N)$

**Exercise 1.2.11.** Show that  $\psi \mapsto [\beta]$  is well-defined, i.e., that  $[\beta]$  is independent of  $\alpha$ .

This defines a map of abelian groups  $\delta_\xi : \text{Hom}_R(M, M) \rightarrow \text{Ext}_R^1(M, N)$  given by  $\varphi \mapsto [\beta]$ . Now, define the homomorphism

$$e : \text{Ext}_R(M, N) \rightarrow \text{Ext}_R^1(M, N), \quad (\xi) \mapsto \delta_\xi(\text{id}_M).$$

Apply  $\text{Hom}_R(M, -)$  to  $(\xi)$  to get the exact sequence

$$0 \rightarrow \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M, T) \rightarrow \text{Hom}_R(M, M).$$

**Claim.** We can extend this sequence to a long exact sequence of abelian groups

$$0 \rightarrow \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M, T) \rightarrow \text{Hom}_R(M, M) \xrightarrow{\delta_\xi} \text{Ext}_R^1(M, N) \rightarrow \text{Ext}_R^1(M, T) \rightarrow \text{Ext}_R^1(M, M).$$

**Exercise 1.2.12.** Show that if  $(\xi)$  is split, then  $\delta_\xi(\text{id}_M) = 0$ .

How is it that  $e$  is injective?

This implies that  $e$  is injective. We need to show that it is surjective as well. Suppose that  $\gamma \in \text{Ext}_R^1(M, N)$  and let  $I_\bullet$  be an injective resolution of  $N$ . Apply  $\text{Hom}_R(M, -)$  to  $I_\bullet$  to get

$$0 \rightarrow \text{Hom}_R(M, N) \xrightarrow{\nu} \text{Hom}_R(M, I_0) \xrightarrow{d_0} \text{Hom}_R(M, I_1) \xrightarrow{d_1} \dots$$



(where we have abused the notation  $d_i$ ). By Proposition 1.2.9(2), we have that  $\gamma = [f]$  for some  $f \in \ker d_1$ . Note that  $f : M \rightarrow \ker \partial_1 = \operatorname{im} \partial_0$ , giving

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & I_0 & \xrightarrow{\partial_0} & \operatorname{im} \partial_0 \longrightarrow 0 \\ & & & & & \uparrow f & \\ & & & & & M & \end{array}$$

where the top row is exact. Take the pullback of  $\partial_0$  and  $f$  to obtain  $T$  such that

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & I_0 & \xrightarrow{\partial_0} & \operatorname{im} \partial_0 \longrightarrow 0 \\ & & \parallel & & \uparrow & & \uparrow f \\ 0 & \longrightarrow & N & \longrightarrow & T & \longrightarrow & M \longrightarrow 0 \end{array}.$$

**Exercise 1.2.13.** Show that the map  $\rho : \operatorname{Ext}_R^1(M, N) \rightarrow \operatorname{Ext}_R(M, N)$  given by  $\gamma \mapsto \xi$  is independent of the choice of  $f$ . Also show that  $\rho$  is inverse to  $e$ .

□

### 1.3 Lecture 3

Let  $N$  be a right  $R$ -module and  $M$  an  $R$ -module. Then  $N \otimes_R M \in \operatorname{ob}(\mathbf{Ab})$  represents the functor  $B_{M,N} : \mathbf{Ab} \rightarrow \mathbf{Ab}$  given by  $A \mapsto \{f : M \times N \rightarrow A \mid f(ax, y) = f(x, ay)\}$ .

**Definition 1.3.1.** Let  $N$  be a right  $R$ -module and  $M$  an  $R$ -module. Let  $x_1, \dots, x_n \in M$ .

- (1) A relation of the  $x_i$ 's with coefficients in  $R$  is a list of scalars  $a_1, \dots, a_n \in R$  such that

$$\sum_{i=1}^n a_i x_i = 0.$$

- (2) A relation of the  $x_i$ 's with coefficients in  $N$  is a list of elements  $y_1, \dots, y_n \in N$  such that

$$\sum_{i=1}^n y_i \otimes x_i = 0.$$

Since  $R \otimes_R M \cong M$ , we see that (1) is a special case of (2).

Let

$$\begin{aligned} a_1 &:= (a_{11}, \dots, a_{1n}) \\ a_2 &:= (a_{21}, \dots, a_{2n}) \\ &\vdots \\ a_m &:= (a_{m1}, \dots, a_{mn}). \end{aligned}$$

be relations of  $x_1, \dots, x_n$  with coefficients in  $R$ . Let  $(z_1, \dots, z_m) \in N^m$ . If  $A$  denotes the matrix  $(a_{ij})$ , then  $y = A^t z \in N^n$  is a relation with coefficients in  $N$ .

**Definition 1.3.2.** A relation  $y$  with coefficients in  $N$  follows from  $R$ -relations if  $y$  is of the form  $A^t z$  for some  $z$  and some matrix  $A$  of relations in  $R$ .

**Lemma 1.3.3.** A right  $R$ -module  $N$  is flat if and only if for any  $R$ -module  $M$  and any  $x_1, \dots, x_n \in M$ , every  $N$ -relation among the  $x_i$  follows from  $R$ -relations.

*Proof.*

( $\implies$ )

We have a module homomorphism  $\varphi : R^n \rightarrow M$  given by  $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i x_i$ . Then

$$\underbrace{\ker \varphi}_K = \{(r_1, \dots, r_n) \in R^n \mid (r_1, \dots, r_n) \text{ is a relation of the } x_i\text{'s in } R\}.$$

We have an exact sequence

$$0 \rightarrow K \xrightarrow{i} R^n \xrightarrow{\varphi} M.$$

If  $N$  is flat, then  $N \otimes_R (-)$  is exact, so that

$$0 \rightarrow N \otimes_R K \xrightarrow{\tilde{i}} N^n \xrightarrow{\tilde{\varphi}} N \otimes_R M$$

is exact. Thus,  $\ker \tilde{\varphi} = (N\text{-relations}) = N \otimes_R K$ .

( $\impliedby$ )

Let  $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$  be a short exact sequence of  $R$ -modules. Since  $N \otimes_R (-)$  is right exact, it suffices to show that

$$N \times_R M' \xrightarrow{\text{id}_N \otimes f} N \otimes_R M$$

is injective. Let  $z \in \ker \text{id}_N \otimes f$ . Then  $z = \sum_{i=1}^n y_i \otimes z_i$ . We know that

$$\sum_{i=1}^n y_i \otimes f(z_i) = \text{id}_N \otimes f(z) = 0,$$

and thus  $(y_1, \dots, y_n)$  is an  $N$ -relation among the  $f(z_i) \in M$ . This shows that there exist  $(a_i^j) \in R$  where  $i = 1, \dots, n$  and  $j = 1, \dots, m$  and elements  $v_1, \dots, v_m \in N$  such that  $y_i = \sum_{j=1}^m v_j a_i^j$ . Therefore,  $\sum_{i=1}^n a_i^j f(z_i) = 0$  for each  $j$ . But  $0 = \sum_{i=1}^n a_i^j f(z_i) = f\left(\sum_{i=1}^n a_i^j z_i\right)$ . As  $f$  is injective, it follows that  $\sum_{i=1}^n a_i^j z_i = 0$  for each  $j$ . Finally, we compute

$$\begin{aligned} \sum_{i=1}^n y_i \otimes z_i &= \sum_{i=1}^n \sum_{j=1}^m (v_j a_i^j) \otimes z_i \\ &= \sum_{j=1}^m v_j \otimes \left( \sum_{i=1}^n a_i^j z_i \right) \\ &= \sum_{j=1}^m (v_j \otimes 0) = 0. \end{aligned}$$

□

**Corollary 1.3.4.**

1. Any free module is flat.
2. Any colimit of flat modules is flat.
3. Any direct summand of a free module is flat, so that any projective module is flat.
4. Any colimit of projective modules is flat.

## 2 Localization

### 2.1 Lecture 4

Let  $R$  be a commutative ring. Given  $x \in R$ , when can we make  $x$  multiplicatively invertible, perhaps in a new ring? This is a question of representability. We have a functor  $\Phi_x : \mathbf{CommRing} \rightarrow \mathbf{Set}$  given by  $B \mapsto \{\varphi : R \rightarrow B \mid \varphi(x) \in B^\times\} \subset \mathrm{Hom}_{\mathbf{CommRing}}(R, B)$ . We are asking whether or not  $\Phi_x$  is representable. That is, we want to find some pair  $(R_x, h)$  where  $R_x$  is a commutative ring and  $h : R \rightarrow R_x$  is a morphism such that  $h(x) \in (R_x)^\times$  and if  $\varphi : R \rightarrow B$  with  $\varphi(x) \in B^\times$ , then  $\varphi = \underline{\varphi} \circ h$  for some map  $\underline{\varphi} : R_x \rightarrow B$ .

In general, we can consider a set  $S$  of nonzero elements and ask for a universal way of making them invertible. But if we make  $S$  invertible, then we will also make the *multiplicative closure*  $\mathrm{cl}(S)$  of  $S$  invertible.

**Definition 2.1.1.** Any  $S \subset R$  is called *multiplicatively closed* if  $0 \notin S$ ,  $1 \in S$ , and  $x, y \in S \implies xy \in S$ .

Given a multiplicatively closed subset  $S \subset R$ , find a universal way of inverting every element of  $S$ . Equivalently, find a ring representing  $\Phi_S$ . Equivalently, find a pair  $(S^{-1}R, h)$  where  $h : R \rightarrow S^{-1}R$  such that  $h(S) \subset (S^{-1}R)^\times$  and any  $\varphi : R \rightarrow B$  with  $\varphi(S) \subset B^\times$  has  $\varphi = \underline{\varphi} \circ h$  for some map  $\underline{\varphi} : S^{-1}R \rightarrow B$ . We call the pair  $(S^{-1}R, h)$  the *localization of  $R$  along  $S$* .

Formally adjoin to  $R$  fractions with numerator in  $R$  and denominator in  $S$ . Consider the set  $(R \times S, \sim)$  where  $(a, s) \sim (b, t)$  if  $u(at - bs) = 0$  for some  $u \in S$ . Set  $S^{-1}R := R \times S / \sim$ . Let  $\frac{a}{s} := [(a, s)]$ . Define

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

and

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Then  $S^{-1}R$  becomes a ring with unity  $\frac{1}{1}$ . Also, we see that  $h : R \rightarrow S^{-1}R$  given by  $a \mapsto \frac{a}{1}$  is a ring homomorphism. Given  $\varphi : R \rightarrow B$  such that  $\mathrm{im} \varphi \subset B^\times$ , we have a well-defined map of rings  $\underline{\varphi} : S^{-1}R \rightarrow B$  given by  $\frac{a}{s} \mapsto \varphi(a)\varphi(s)^{-1}$ , which satisfies  $\underline{\varphi} \circ h = \varphi$ .

**Example 2.1.2.** Here are some natural choices for  $S$ .

- (a)  $S = \{1, x, x^2, \dots\}$  with  $x$  not nilpotent.
- (b)  $S = R^\times$ .

(c)  $S = \{r \in R : r \text{ is not a zero divisor.}\}.$

If  $A$  is an integral domain and we take any multiplicatively closed subset  $S \subset A$ , then  $\text{Frac}(A) := (A \setminus \{0\})^{-1}A$  is a field and  $h : A \rightarrow (A \setminus \{0\})^{-1}A$  is injective. For now, let  $S$  denote the set of non zero-divisors. If  $\frac{a}{b} \in \text{Frac}(A)$  is nonzero, then  $\frac{a}{b} \neq \frac{0}{1}$ , i.e.,  $a \cdot 1$  is not a zero divisor, so that  $a \neq 0$  and thus  $\frac{b}{a} \in \text{Frac}(A)$ . This shows that  $\text{Frac}(A)$  is a field. Moreover, if  $a \in A$  has  $h(a) = \frac{a}{1} = 0 \in \text{Frac}(A)$ , then  $\frac{a}{1} = \frac{0}{1} \implies a \cdot 1$  is a zero divisor. Hence  $a = 0$ , and  $h$  is injective.

If  $S$  is generic, then  $S^{-1}A \subset \text{Frac}(A)$  since  $S^{-1}A$  equals the subring generated by  $A \cong h(A)$  and  $S^{-1} = \{\frac{1}{s} \mid s \in S\}$ . In this case,  $(S^{-1}A, h)$  represents the functor  $\Phi : \mathbf{Field} \rightarrow \mathbf{Set}$  given by  $k \mapsto \{\varphi : A \rightarrow k \mid \varphi \text{ is injective.}\}$ . This means that for any ring map  $\varphi : A \rightarrow B$  with  $\varphi(S) \subset B^\times$ , there is some unique map  $\psi$  such that  $\psi \circ h = \varphi$ .

## 2.2 Lecture 5

### Example 2.2.1.

1. If  $S = \{1, x, x^2, \dots\}$  with  $x$  not nilpotent, then  $S^{-1}A = A_f \equiv \left\{ \frac{a}{f^n} : n \geq 0, a \in A \right\}$ .
2. If  $S \subset A^\times$ , then  $h : A \rightarrow S^{-1}A$  is an isomorphism.
3. If  $A$  is any ring and  $S \subset A$  denotes the set of all non-zero divisors, then  $\text{Frac}(A) = S^{-1}A$  is called the *fraction ring* of  $A$ . If  $A$  is an integral domain, then  $\text{Frac}(A)$  is a field and  $H : A \rightarrow \text{Frac}(A)$  is injective. In this cases,  $(\text{Frac}(A), h)$  represents the functor  $F_A : \mathbf{Field} \rightarrow \mathbf{Set}$  given by  $K \mapsto \{\varphi : A \rightarrow K \mid \varphi \text{ monomorphism}\}.$

Let  $A$  be a commutative ring and  $S \subset A$  be multiplicatively closed. Let  $M$  be an  $A$ -module. Define the equivalence relation  $(M \times S, \sim)$  where  $(m, s) \sim (n, t)$  if  $u(tm - sn) = 0$  for some  $u \in S$ . Define the  $A$ -module  $S^{-1}M = M \times S / \sim$  where  $\frac{m}{s} + \frac{n}{t} := \frac{tm + sn}{st}$ . Define the module homomorphism  $h_M : M \rightarrow S^{-1}M$  by  $m \mapsto [(m, 1)]$ . Let  $\frac{m}{s}$  denote the equivalence class  $[(m, s)]$ .

Moreover,  $S^{-1}M$  is naturally a module over  $S^{-1}A$  via the action  $\frac{a}{s} \cdot \frac{m}{t} := \frac{a \cdot m}{st}$ . This makes  $h_M$  a module over  $h : A \rightarrow S^{-1}A$  in that for any  $a \in A$  and  $m \in M$ , we have that  $h_M(a \cdot m) = h(a) \cdot h_M(m)$ .

We see that  $S^{-1}(-)$  is a functor which maps each homomorphism  $\varphi : M \rightarrow N$  to  $S^{-1}\varphi : S^{-1}M \rightarrow S^{-1}N$  given by  $\frac{m}{s} \mapsto \frac{\varphi(m)}{s}$ . It's easy to verify that  $S^{-1}(-)$  is left adjoint to the pullback functor  $h^\bullet$ .

If  $f : A \rightarrow B$  is a map of **commutative** rings, then there are natural functors  $f^\bullet : B\text{-}\mathbf{Mod} \rightarrow A\text{-}\mathbf{Mod}$  and  $f_\bullet : A\text{-}\mathbf{Mod} \rightarrow B\text{-}\mathbf{Mod}$ , called the *pullback* and *pushforward*, respectively.

On the one hand, the pullback functor is already familiar to us. On the other hand, the pushforward acts on objects by

$$f_\bullet(M) \equiv B \otimes_A M$$

where  $B$  is viewed as an  $A$ -module via  $f$  along with the action  $b \cdot (c \otimes m) \equiv (bc) \otimes m$ . It acts on morphisms by  $(\varphi : M \rightarrow N) \mapsto (\text{id}_B \otimes \varphi : f_\bullet(M) \rightarrow f_\bullet(N))$ .

**Exercise 2.2.2.**  $(f_\bullet, f^\bullet)$  is an adjoint pair.

**Corollary 2.2.3.**  $S^{-1}(-) \cong h_{\bullet}$ .

Naively, we could have tried to define fractions in  $A$  by  $(a, s) \sim_n (b, t)$  if  $(at - bs = 0)$ . But this is not in general an equivalence relation, for it is not transitive. Indeed, set  $A = \mathbb{C}[x, y]_{(xy)}$  and  $S = \{1, x, x^2, \dots\}$ . Consider the localization  $A_x$ . Note that  $(y, 1) \not\sim_n (0, 1)$  but that  $(y, 1) \sim_n (0, x)$  and  $(0, x) \sim_n (0, 1)$ .

**Note 2.2.4.** We have that  $A_x = \mathbb{C}[x, x^{-1}]$ , which is a field, and that  $h : A \rightarrow A_x$  is given by

$$\underbrace{[f(x, y)]}_{[p(x)+yq(y)]} \mapsto p(x),$$

which is non-injective.

**Proposition 2.2.5.**

1. If  $h : A \rightarrow S^{-1}A$ , then  $\ker h = \{a \in A : (\exists s \in S) (sa = 0)\}$ .
2.  $S^{-1}A$  is flat as an  $A$ -module.

**Corollary 2.2.6.**  $S^{-1}(-)$  is an exact functor.

*Proof.* Let  $M \xrightarrow{f} T \xrightarrow{g} N$  be an exact sequence of  $A$ -modules. We want to show that

$$S^{-1}M \xrightarrow{S^{-1}f} S^{-1}T \xrightarrow{S^{-1}g} S^{-1}N$$

is exact as well. Let  $\frac{x}{s} \in S^{-1}T$  with  $(S^{-1}g)\left(\frac{x}{s}\right) = 0$ . This implies that  $\frac{g(x)}{s} = \frac{0}{1}$ , so that  $ug(x) = 0$  for some  $u \in S$ . But since  $g$  is a morphism, we know that  $0 = ug(x) = g(ux)$ . This means that  $f(y) = ux$  for some  $y \in M$ . Then  $\frac{y}{us} \in S^{-1}M$  such that  $(S^{-1}f)\left(\frac{y}{us}\right) = \frac{f(y)}{us} = \frac{ux}{us} = \frac{x}{s}$ .  $\square$

Suppose that  $f \in A$  is not nilpotent. We can compute  $A_f$  explicitly as follows. There is a natural map  $A_f[x] \rightarrow A_f$  given by  $x \mapsto \frac{1}{f}$ . This induces  $A_f[x]_{\left(x - \frac{1}{f}\right)} \xrightarrow{\cong} A_f$ . We also have a map  $A[x] \rightarrow A_f[x]$  from the map  $h$  on the coefficients. Define the map  $\alpha : A[x] \rightarrow A_f$  by  $a \mapsto h(a) = \frac{a}{1}$  and  $x \mapsto \frac{1}{f}$ . We must compute  $\ker \alpha$  as an ideal in  $A[x]$ . This is surjective since any element in  $A_f$  is of the form  $\frac{a}{f^n}$  for some  $a \in A$  and  $n \in \mathbb{N}$ , so that  $ax^n \mapsto \frac{a}{f^n}$ .

## 2.3 Lecture 6

**Claim.**  $\ker \alpha = (fx - 1)$ .

*Proof.* Note that  $xf - 1 \in \ker \alpha$ . Also, note that  $\exists n \geq 0. f^n g\left(\frac{1}{f}\right) = 0 \iff \alpha(g) = 0 \iff g\left(\frac{1}{f}\right) = 0$  in  $A_f$ . Without loss of generality, we may assume that  $n \geq \deg g$ . Thus,  $f^n g(x)$  is a polynomial of  $fx$  with coefficients in  $A$ , so that there is some  $G(y) \in A[y]$  such that  $G(fx) = f^n g(x)$ . Then  $g \in \ker \alpha \iff \exists G(y) \in A[y]. G(fx) = f^n g(x) \wedge G(1) = 0$ . But then  $G(y) = (y - 1)h(y)$  where  $h(y) \in A[y]$ . This implies that  $g(x) \in \ker \alpha \iff \exists n \geq 0. f^n g(x) \in (xf - 1)$ . But  $f, fx - 1 \in A[x]$  are

relatively prime since  $1 = fx + (fx - 1)(-1)$ . Hence  $1^n = (fx + (fx - 1)(-1))^n = f^n x^n + (fx - 1)s(x)$  for some  $s(x) \in A[x]$ . Multiply by  $g(x)$  to get

$$g(x) = \underbrace{f^n g(x)}_{\in (xf-1)} + \underbrace{(fx-1)s(x)g(x)}_{\in (xf-1)}.$$

Therefore,  $g(x) \in (xf - 1)$ , and  $(xf - 1) = \ker \alpha$ .  $\square$

Suppose that  $\varphi : A \rightarrow B$  is a map of commutative rings. Then we can transport the ideals along  $\varphi$  as follows.

**Definition 2.3.1.**

1. Given an ideal  $\mathfrak{a} \trianglelefteq A$ , the *extension of  $\mathfrak{a}$  along  $\varphi$*  is the ideal  $\mathfrak{a}^e \trianglelefteq B$  that is generated by  $\varphi(\mathfrak{a})$ , i.e.,  $\mathfrak{a}^e = \varphi(\mathfrak{a}) \cdot B$ .
2. Given an ideal  $\mathfrak{b} \trianglelefteq B$ , the *contraction of  $\mathfrak{b}$  along  $\varphi$*  is defined as the ideal  $\mathfrak{b}^c = \varphi^{-1}(\mathfrak{b})$ .

Suppose that  $A$  is a commutative ring and that  $S \subset A$  is multiplicatively closed. Recall the map  $h : A \rightarrow S^{-1}A$ . We want to study  $(-)^e$  and  $(-)^c$  along  $h$ .

**Proposition 2.3.2.**

1. If  $\mathfrak{a} \trianglelefteq A$ , then  $\mathfrak{a}^e = \left\{ \frac{a}{s} \mid a \in \mathfrak{a}, s \in S \right\}$ .

*Proof.* By definition,  $\mathfrak{a}^e = h(\mathfrak{a}) \cdot S^{-1}A = \left\{ \sum_i \frac{b_i}{t_i} \frac{a_i}{s_i} \mid a_i \in \mathfrak{a}, b_i \in A, s_i, t_i \in S \right\}$ . Since  $a_i b_i \in \mathfrak{a}$  and  $s_i t_i \in S$ , our proof is complete.  $\square$

2. If  $\mathfrak{a} \trianglelefteq A$ , then  $\mathfrak{a}^e = (1) \iff \mathfrak{a} \cap S \neq \emptyset$ .

*Proof.* Note that  $(S^{-1}A)^\times$  consists of every fraction  $\frac{a}{s}$  for which we can find some fraction  $\frac{b}{t}$  such that  $\frac{a}{s} \frac{b}{t} = 1$ . Therefore, we must have some element  $u \in S$  such that  $u(ab - st) = 0 \iff \exists \beta \in A, \beta a \in S$ . Thus,  $(S^{-1}A)^\times = \left\{ \frac{a}{s} \mid \exists \beta \in A, \beta a \in S \right\}$ . But then  $\mathfrak{a}^e = (1) \iff \mathfrak{a}^e$  contains some unit  $\iff \exists \frac{a}{s} \in \mathfrak{a}^e, \exists \beta \in A, \beta \cdot a \in S \iff \beta \cdot a \in S \cap \mathfrak{a}$ .  $\square$

3. Suppose that  $I \trianglelefteq S^{-1}A$  is an ideal. Then we can form  $I^{ce} \trianglelefteq S^{-1}A$ . By definition,  $I \supset I^{ce}$ . In fact,  $I = I^{ce}$ .

*Proof.* If  $\frac{a}{s} \in I$ , then  $a \in h^{-1}(I)$  because  $h^{-1}(I) = \{r \in A \mid \frac{r}{1} \in I\}$ . But  $\frac{a}{1} = s \cdot \frac{a}{s}$  where  $s \in S^{-1}A$  and  $\frac{a}{s} \in I$ , so that  $a \in I$ . This implies that  $\frac{a}{s} \in I^{ce}$  for each  $s \in S$ , and thus  $I \subset I^{ce}$ .  $\square$

4. If  $\mathfrak{a} \trianglelefteq A$ , then  $\mathfrak{a}^{ec} = \{r \in A \mid \exists s \in S, sr \in \mathfrak{a}\}$ .

*Proof.* Suppose that  $a \in \mathfrak{a}^{ec}$ . Then  $\frac{a}{1} = h(a) \in \mathfrak{a}^e$ , so that  $\exists b \in \mathfrak{a}, \exists s \in S, \frac{a}{1} = \frac{b}{s}$ . This implies that  $\exists u \in S$  such that  $u(sa - b) = 0$ . Hence  $(us)a = b$ , and  $\mathfrak{a}^{ec} \subset \{r \in A \mid \exists s \in S, sr \in \mathfrak{a}\}$ . If  $r \in A$  is such that  $rs \in \mathfrak{a}$  for some  $s \in S$ , then  $\frac{r}{1} = \frac{rs}{s} \in \mathfrak{a}^e$  and thus  $r \in \mathfrak{a}^{ec}$ .  $\square$

5. We have that  $\mathfrak{a} \trianglelefteq A$  is contracted (i.e.,  $\mathfrak{a} = I^c$  for some  $I \trianglelefteq S^{-1}A$ ) if and only if  $\mathfrak{a} = \mathfrak{a}^{ec}$  if and only if  $[s] \in A/\mathfrak{a}$  is not a zero divisor for any  $s \in S$ .
6. The map  $(-)^e$  induces a bijection  $(-)^e : \{\mathfrak{a} \trianglelefteq A \mid \mathfrak{a} \text{ is a contraction of some ideal}\} \rightarrow \{I \mid I \trianglelefteq S^{-1}A\}$  that preserves inclusions of ideals.

Suppose that  $M$  is an  $A$ -module.

**Definition 2.3.3.** A submodule  $N \subset M$  is  $S$ -saturated if  $N = \{x \in M \mid (\exists s \in S)(sx \in N)\}$ .

If  $M = A$  and  $N = \mathfrak{a}$ , then  $N$  is  $S$ -saturated if and only if  $\mathfrak{a} = \mathfrak{a}^{ec}$ . The localization on modules induces an inclusion-preserving bijection

$$S^{-1}(-) : \{N \subset M \mid N \text{ is } S\text{-saturated}\} \rightarrow \{M \mid M \subset S^{-1}M\}.$$

**Exercise 2.3.4.** An ideal  $\mathfrak{b} \trianglelefteq A$  is prime if and only if  $A \setminus \mathfrak{b}$  is multiplicatively closed.

## 2.4 Lecture 7

**Proposition 2.4.1.** If  $\mathfrak{p} \trianglelefteq A$  is prime and  $S \subset A$  is multiplicatively closed, then  $\mathfrak{p}^e \trianglelefteq S^{-1}A$  is prime if and only if  $S \cap \mathfrak{p} = \emptyset$ .

*Proof.* The forward direction is obvious. Conversely, suppose that  $S \cap \mathfrak{p} = \emptyset$ . Then  $\mathfrak{p}^{ec} = \mathfrak{p}$ . Indeed,  $\mathfrak{p}^{ec} = \{a \in A \mid \exists s \in S, sa \in \mathfrak{p}\}$ . But if  $sa \in \mathfrak{p}$ , then either  $s \in \mathfrak{p}$  or  $a \in \mathfrak{p}$ . Since  $S \cap \mathfrak{p} = \emptyset$ , we see that  $s \notin \mathfrak{p} \implies a \in \mathfrak{p}$ . Suppose that  $x \cdot y \in \mathfrak{p}^e$ . Then  $x = \frac{a}{s}$  for some  $a \in A$  and  $s \in S$ , and  $y = \frac{b}{t}$  for some  $b \in A$  and  $t \in B$ . Then  $\frac{ab}{st} \in \mathfrak{p}^e$ , so that  $\frac{ab}{t} \in \mathfrak{p}^e$  since  $\mathfrak{p}^e$  is an ideal. Hence  $ab \in \mathfrak{p}$ , which is prime by assumption. Say that  $a \in \mathfrak{p}$ . Then  $\frac{a}{s} \in \mathfrak{p}^e$ .  $\square$

**Corollary 2.4.2.** If  $S \subset A$  is multiplicatively closed, then we get a bijection

$$\{\mathfrak{p} \in \text{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\} \xrightarrow{(-)^e} \text{Spec}(S^{-1}A).$$

*Proof.* This is because  $\mathfrak{p}^c$  is prime in  $A$  with  $\mathfrak{p}^c \cap S = \emptyset$  whenever  $\mathfrak{p}$  is prime in  $S^{-1}A$ .  $\square$

Now, recall the property P that an ideal  $\mathfrak{a}$  in  $A$  is prime if and only if  $A \setminus \mathfrak{a}$  is multiplicatively closed.

**Proposition 2.4.3.**  $\mathfrak{a}$  is prime if and only if there is some multiplicatively closed  $S \subset A$  such that  $S \cap \mathfrak{a} = \emptyset$  and  $\mathfrak{a}$  is maximal among all ideals satisfying P.

*Proof.* If  $\mathfrak{a}$  is prime, then  $S = A \setminus \mathfrak{a}$  is multiplicatively closed and  $\mathfrak{a}$  is maximal. Conversely, let  $a, b \in A$  such that  $a, b \notin \mathfrak{a}$ . We must show that  $ab \notin \mathfrak{a}$ . Consider  $\mathfrak{a} + (a) \supsetneq \mathfrak{a}$  and  $\mathfrak{a} + (b) \supsetneq \mathfrak{a}$ . But we are given  $S$  such that  $\mathfrak{a} \cap S = \emptyset$ . Hence there are  $s \in S \cap (\mathfrak{a} + (a))$  and  $t \in S \cap (\mathfrak{a} + (b))$ . Then  $s = \alpha + x \cdot a$  and  $t = \beta + y \cdot b$  where  $\alpha, \beta \in \mathfrak{a}$  and  $x, y \in A$ . We compute

$$st = \alpha\beta + \alpha yb + \beta xa + xyab,$$

where  $st \in S$  and  $\alpha\beta, \alpha yb, \beta xa \in \mathfrak{a}$ . If we assume that  $ab \in \mathfrak{a}$ , then  $st \in S \cap \mathfrak{a}$ , a contradiction.  $\square$

**Note 2.4.4.** If  $S \subset A$  is multiplicatively closed, then by Zorn's lemma there is some prime ideal  $\mathfrak{b}$  such that  $\mathfrak{b} = A \setminus S$ .

**Definition 2.4.5.** Let  $A$  be a ring. We call  $A$  a *local ring* if any of the following equivalent conditions holds.

- (a)  $A$  has a unique maximal ideal  $\mathfrak{m}$ .
- (b)  $A \setminus A^\times$  is an ideal.
- (c) If  $\mathfrak{m}$  is maximal and  $x \in \mathfrak{m}$ , then  $1 + x \in A^\times$ .

If  $A$  is a ring and  $\mathfrak{p}$  a prime ideal, we will denote the localization  $(A - \mathfrak{p})^{-1}A$  by  $A_{\mathfrak{p}}$ .

**Proposition 2.4.6.** If  $\mathfrak{p}$  is prime, then  $A_{\mathfrak{p}}$  is a local ring with unique maximal ideal  $\mathfrak{p}^e$ .

*Proof.* Let  $S = A \setminus \mathfrak{p}$ . Then  $A_{\mathfrak{p}} = S^{-1}A$ . Suppose that  $I \trianglelefteq A_{\mathfrak{p}} = S^{-1}A$  such that  $I \neq (1)$ . But any ideal in  $S^{-1}A$  is of the form  $I = \mathfrak{a}^e$  for some ideal  $\mathfrak{a}$  in  $A$ . Since  $(1) \neq I = \mathfrak{a}^e$ , it follows that  $\mathfrak{a} \cap S = \emptyset$ . Therefore,  $\mathfrak{a} = A \setminus S = \mathfrak{p}$ , so that  $I = \mathfrak{a}^e \subset \mathfrak{p}^e$ . Hence every nontrivial ideal in  $A_{\mathfrak{p}}$  is contained in  $\mathfrak{p}^e$ , implying that  $\mathfrak{p}^e$  is the unique maximal ideal.  $\square$

**Corollary 2.4.7.** In particular, the map

$$(\text{prime ideal of } A \mid A \subset \mathfrak{p}) \xrightarrow{(-)^e} \text{Spec}(A_{\mathfrak{p}})$$

is a bijection that preserves inclusions of ideals.

**Definition 2.4.8.** If  $A$  is a commutative ring, then for every  $\mathfrak{p} \trianglelefteq A$  prime, we define the *height* of  $\mathfrak{p}$  as

$$\text{ht}(\mathfrak{p}) \equiv \sup\{k \mid \mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_k, \mathfrak{p}_i \trianglelefteq A\}.$$

Note that  $\text{ht}(\mathfrak{p}) = \text{ht}(\mathfrak{p}^e \text{ in } A_{\mathfrak{p}})$ .

**Definition 2.4.9.** The *Krull dimension* of  $A$  is

$$\dim A \equiv \sup\{\text{ht}(\mathfrak{m}) \mid \text{maximal } \mathfrak{m} \trianglelefteq A\}.$$

Note that  $\dim A_{\mathfrak{p}} = \text{ht}(\mathfrak{p})$  and that  $\dim A = \sup\{\dim A_{\mathfrak{m}} \mid \text{maximal } \mathfrak{m} \trianglelefteq A\}$ .

**Example 2.4.10.**

1. If  $k$  is a field, then  $\dim k = 0$ . (The converse is also true.)
2. If  $A$  is a PID, then  $\dim A = 1$ . For example,  $\mathbb{Z}$ ,  $\mathbb{Q}[x]$ , and  $\mathbb{Z}[i]$  have dimension 1.

**Exercise 2.4.11.**

1. Show that  $\mathbb{Z}[-\sqrt{5}]$  is not a PID but has dimension 1.
2. Show that  $\dim \mathbb{C}[x_1, \dots, x_n] = n$ .



### 3 Basic algebraic geometry

Any information about  $A$ , any prime ideal in  $A$ , any localization in  $A$ , and their relations can be packaged in a geometrical entity, specifically, a topological space along with a distinguished class of maps.

Let  $X = \text{Spec}(A)$ , the set of all prime ideals in  $A$ , or *spectrum of  $A$* . For any  $f \in A$ , define the *principal open subset associated with  $f$*  as

$$X_f \equiv \{\mathfrak{p} \in X \mid f \notin \mathfrak{p}\}.$$

Such subsets satisfy

- (a)  $X_f \cap X_g = X_{fg}$ .
- (b)  $X_{f^n} = X_f$ ,  $X_f = X \iff f \notin \mathfrak{p} \forall \mathfrak{p} \text{ prime} \iff f \in A^\times$ .
- (c)  $X_f = \emptyset \iff f \in \bigcap_{\mathfrak{p} \in X} \mathfrak{p}$ .

**Definition 3.0.1.** The minimal topology on  $X$  generated by  $\{X_f\}_{f \in A}$  is called the *Zariski topology* on  $X$ .

The subset  $U \subset X$  is open if and only if there is some  $T \subset A$  such that  $U = \bigcup_{f \in T} X_f$ . Also,  $Y \subset X$  is closed if  $Y = \bigcap_{f \in T} (X \setminus X_f)$  for some  $T \subset A$ . Hence  $Y \subset X$  is closed if there is some  $T \subset A$  such that

$$Y = \{\mathfrak{p} \mid \mathfrak{p} \supset \langle T \rangle\}.$$

In particular, for any ideal  $\mathfrak{a} \leq A$ , we can define a Zariski-closed subset  $V(\mathfrak{a}) = \{\mathfrak{p} \in X \mid \mathfrak{p} \supset \mathfrak{a}\}$ . (Note that replacing  $\mathfrak{a}$  with a set  $S \subset A$  determines an equivalent topology.) Every closed subset is of this form.

**Exercise 3.0.2.** Write arbitrary intersections of closed sets, finite unions of closed sets,  $X$ , and  $\emptyset$  in this form.

Any  $f \in A$  can be viewed as a function on  $X$  in two ways. First, view  $f$  as a mapping  $X \rightarrow \prod_{\mathfrak{p} \in X} A_{\mathfrak{p}}$  given by  $\mathfrak{p} \mapsto \frac{f}{1} \in A_{\mathfrak{p}}$ . Then for any  $\mathfrak{p}$ , the value of  $f$  on  $\mathfrak{p}$  is in  $A_{\mathfrak{p}}$ . Second, view  $f$  as a mapping  $X \rightarrow \prod_{\mathfrak{p} \in X} k_{\mathfrak{p}}$  given by

$$f \mapsto \frac{f}{1} + \mathfrak{p}^e \in k_{\mathfrak{p}} = A_{\mathfrak{p}}/\mathfrak{p}^e.$$

We call  $k_{\mathfrak{p}}$  the *residue field of  $A_{\mathfrak{p}}$* .

**Example 3.0.3.** Suppose that  $k$  is a field and  $A = k[x_1, \dots, x_n]$  such that for any  $\mathfrak{m}$ ,  $k_{\mathfrak{m}} = k$ . Then  $f \in A$  induces a function (prime ideals in  $A$ )  $\rightarrow k$  given by  $(x_1 - a_1, \dots, x_n - a_n) \mapsto f(a_1, \dots, a_n)$ .

**Lemma 3.0.4.**  $X$  is quasi-compact, meaning that for any Zariski-open  $U \subset X$  and any open cover  $\{U_{\alpha}\}$  of  $X$ , there is some finite subcover and  $U = \bigcup_{\alpha} U_{\alpha}$ .

**Note 3.0.5.**  $X$  is not Hausdorff in general.

**Exercise 3.0.6.** Let  $A = \mathbb{C}[x]$ . Show that  $X = \text{Spec}(A)$  is not Hausdorff.

### 3.1 Lecture 8

#### Note 3.1.1.

1. We have that  $V(S) = V(\mathfrak{a})$  when  $\mathfrak{a} = \langle S \rangle$ .
2. The Zariski topology is generated by the collection of principal open subsets on  $X$ , i.e., subsets of the form  $X_f = \{\mathfrak{b} \in X \mid f \notin \mathfrak{b}\}$  where  $f \in A$ . The elements in the ring  $A$  may be viewed as kinds of functions on  $X$ . View  $f \in A$  as a function  $X \rightarrow \coprod_{\mathfrak{b} \in X} A_{\mathfrak{b}} \rightarrow \coprod_{\mathfrak{b} \in X} A + \mathfrak{b}/\mathfrak{b}^c$  defined by  $\mathfrak{b} \mapsto \frac{f}{1} \in A_{\mathfrak{b}}$ .

If  $k$  is a field and  $A = k[x_1, \dots, x_n]$ , then  $V(a_1, \dots, a_n) \in A^n$ . We get a maximal ideal

$$\langle x_1 - a_1, x_2 - a_2, \dots, x_n - a_n \rangle.$$

Thus, if  $f(x) \in A$  and we restrict this function, then we get the evaluation of  $f$  on points  $a \in A^n$ .

$$\begin{array}{ccc} a \xrightarrow{\epsilon} \langle x_1 - a_1, x_2 - a_2, \dots, x_n - a_n \rangle X & \longrightarrow & \coprod_{\mathfrak{b}} k_{\mathfrak{b}} \\ \uparrow & & \uparrow \\ A^n & \longrightarrow & \coprod_a k \cong A^n \times k \end{array}$$

This geometric way of packaging information about  $A$  and all of its prime ideals is compatible with all natural rings homomorphisms between the  $A_p$ 's. If we have a principal open, then for every  $f \in A$ , we get a ring  $A_f$ , provided that  $f$  is not nilpotent, and a functor (poset of principal open sets in  $X$ )<sup>op</sup>  $\rightarrow$  **CommRing** given by  $X_f \mapsto A_f$ . This extends to another functor (opens in  $X$ )<sup>op</sup>  $\rightarrow$  **CommRing**. Given  $f \in A$ , viewing  $f$  as a kind of function on  $X$  thus induces a compatible system of elements of all rings  $A(U)$  where  $U \in X$  is open.

**Lemma 3.1.2.**  *$X$  is quasi-compact, meaning that any open cover  $\{U_{\alpha}\}$  of  $X$  admits some finite subcover.*

*Proof.* Let  $X = \bigcup_{\alpha} U_{\alpha}$ . The principal opens generate the Zariski topology, so that for any  $\alpha$ , we can find a cover  $U_{\alpha} = \bigcup_{\beta} X_{f_{\alpha}^{\beta}}$  where  $f_{\alpha}^{\beta} \in A$ . Then  $X = \bigcup_{\alpha, \beta} X_{f_{\alpha}^{\beta}}$ , so that

$$\emptyset = \bigcap_{\alpha, \beta} \underbrace{(X - X_{f_{\alpha}^{\beta}})}_{V(f_{\alpha}^{\beta})}.$$

But  $\emptyset = \bigcap_{\alpha, \beta} V(f_{\alpha}^{\beta}) = V(\{f_{\alpha}^{\beta}\}_{\alpha, \beta})$ . Hence  $\langle (f_{\alpha}^{\beta})_{\alpha, \beta} \rangle$  is not contained in any prime ideal, so that  $\langle (f_{\alpha}^{\beta})_{\alpha, \beta} \rangle = A$ , hence  $1 \in \langle (f_{\alpha}^{\beta})_{\alpha, \beta} \rangle$ . We can find a collection of elements  $\{a_{\alpha}^{\beta}\}_{\alpha, \beta}$  where  $a_{\alpha}^{\beta} \in A$  such that  $1 = \sum_{\alpha, \beta} a_{\alpha}^{\beta} f_{\alpha}^{\beta}$  and at most finitely many  $a_{\alpha}^{\beta}$  are nonzero. Thus, there is sequence  $(\alpha_1, \beta_1), \dots, (\alpha_k, \beta_k)$  with

$$\langle f_{\alpha_1}^{\beta_1}, \dots, f_{\alpha_k}^{\beta_k} \rangle = \langle 1 \rangle = A.$$

Hence  $V(f_{\alpha_1}^{\beta_1}) \cap \dots \cap V(f_{\alpha_k}^{\beta_k}) = \emptyset$ , and  $X = X_{f_{\alpha_1}^{\beta_1}} \cup \dots \cup X_{f_{\alpha_k}^{\beta_k}}$ . But  $X_{f_{\alpha_i}^{\beta_i}} \in U_{\alpha_i}$  for each  $i = 1, \dots, k$ . Therefore,  $X = U_{\alpha_1} \cup \dots \cup U_{\alpha_k}$ .  $\square$

**Example 3.1.3.** Suppose that  $X$  is a compact and Hausdorff space. Let  $A = C(X)$ , the ring of complex-valued continuous functions on  $X$ . Consider  $\text{Spec}(A)$  equipped with the Zariski topology and its subset  $\text{Max}(A) := \{\mathfrak{a} \in C(X) \mid \mathfrak{a} \text{ maximal}\}$  equipped with the subspace topology.

**Claim.** *The natural map  $X \xrightarrow{\varphi} \text{Max}(A)$  given by  $x \mapsto \{f \in C(X) \mid f(x) = 0\}$  is a homeomorphism.*

*Proof.* Let  $\mathfrak{a}_x := \ker(\text{ev}_x : A \rightarrow \mathbb{C})$ . By Urysohn's lemma, for any two distinct points  $x, y \in X$ , there is some  $f \in A$  such that  $f(x) = 0$  and  $f(y) = 1$ . But  $f \in \mathfrak{a}_x$  and  $f \notin \mathfrak{a}_y$ , making  $\mathfrak{a}_x \neq \mathfrak{a}_y$ . Now, suppose  $\mathfrak{a} \in \text{Max}(A)$  and  $\mathfrak{a} \neq \mathfrak{a}_x$  for any  $x \in X$ . This means that for any  $x \in X$ , there is some  $f_x \in \mathfrak{a}$  such that  $f_x(x) \neq 0$ . Let  $U_x \subset U$  be an open neighborhood of  $x \in X$  such that  $f_x|_{U_x} \neq 0$ . Then  $X = \bigcup_{x \in X} U_x$ , so that there is some finite subcover  $U_{x_1}, \dots, U_{x_k}$  of  $X$ . Let  $f = \sum_{i=1}^k |f_{x_i}|^2$ , which does not vanish at any point of  $X$ . Note that  $f = \sum_{i=1}^k f_{x_i} \cdot \bar{f}_{x_i}$ , so that  $f \in \mathfrak{a}$ . But  $f$  is nowhere vanishing, so that  $\frac{1}{f}$  is a well defined continuous function on  $X$ . Thus,  $\frac{1}{f} \in A$ , and  $1 \in \mathfrak{a}$ , contrary to the fact that  $\mathfrak{a}$  is maximal.

**Exercise 3.1.4.** *Check that  $\varphi$  is continuous, hence a homeomorphism.*

□

Let  $A$  be a commutative ring and  $M$  an  $A$ -module. Then  $M$  defines a subset of  $X := \text{Spec}(A)$ , namely

$$\text{supp}(M) \equiv \{\mathfrak{b} \in X \mid M_{\mathfrak{b}} \neq 0\},$$

called the *support* of  $M$ .

**Proposition 3.1.5.**

1.  $\text{supp}(M) \subset V(\text{ann}(M))$  where  $\text{ann}(M) \equiv \{a \in A \mid a \cdot m = 0 \text{ for each } m \in M\}$ .

*Proof.* Let  $\mathfrak{b} \in \text{supp}(M)$ . Then  $M_{\mathfrak{b}} \neq (0)$ . We need to show that  $\text{ann}(M) \subset \mathfrak{b}$ . Suppose that there is some  $a \in \text{ann}(M)$  with  $a \notin \mathfrak{b}$ . Let  $x \in M_{\mathfrak{b}}$ . Then  $x = \frac{m}{s}$  where  $m \in M$  and  $s \notin \mathfrak{b}$ . We compute  $\frac{a}{1} \cdot \frac{m}{s} = \frac{am}{s} = 0$  in  $M_{\mathfrak{b}}$ . Since  $a \notin \mathfrak{b}$ , it follows that  $\frac{a}{1}$  is invertible in  $A_{\mathfrak{b}}$ , i.e.,  $\frac{1}{a} \in A_{\mathfrak{b}}$ . Hence  $\frac{m}{s} = \frac{1}{a} \left( \frac{a}{1} \frac{m}{s} \right) = 0$  in  $M_{\mathfrak{b}}$ , so that  $M_{\mathfrak{b}} = (0)$ , a contradiction. □

2. *If  $M$  is finitely generated, then  $\text{supp}(M) \supset V(\text{ann}(M))$ .*

*Proof.* Let  $\mathfrak{b} \in V(\text{ann}(M))$  and  $\mathfrak{b} \supset \text{ann}(M)$ . We want to show that  $M_{\mathfrak{b}} \neq (0)$ . Suppose to the contrary. Then for any  $m \in M$  we have that  $\frac{m}{1} = 0$  in  $M_{\mathfrak{b}}$ . This shows that there exists  $s \notin \mathfrak{b}$  such that  $s \cdot m = 0$  in  $M$ . But  $M$  is finitely generated. Let  $m_1, \dots, m_k \in M$  be generators of  $M$ . Then there are  $s_1, \dots, s_k \in A \setminus \mathfrak{b}$  such that  $s_i m_i = 0$  in  $M$  for each  $i$ . Let  $s = s_1 \cdots s_k \in A \setminus \mathfrak{b}$ . Then for any  $m \in M$ , we have that  $s \cdot m = 0$ . Hence  $s \in \text{ann}(M)$ , a contradiction. □

### 3.2 Lecture 9

**Proposition 3.2.1.**  $M = (0) \iff \text{supp}(M) = \emptyset \iff \text{supp}(M) \cap \text{Max}(A) = \emptyset$ .

*Proof.* It's clear that  $M = \emptyset \implies \text{supp}(M) = (0) \implies \text{supp}(M) \cap \text{Max}(A) = \emptyset$ . Hence it suffices to show that

$$\text{supp}(M) \cap \text{Max}(A) = \emptyset \implies M = (0).$$

On the one hand, if  $M$  is finitely generated, then  $\text{supp}(M) = V(\text{ann}(M))$ , so that  $\text{supp}(M)$  must contain any maximal ideal that contains  $\text{ann}(M) \leq A$ . Thus, the assumption that  $\text{supp}(M) \cap \text{Max}(A) = \emptyset$  implies that  $\text{ann}(M)$  is not contained in any maximal ideal, meaning that  $\text{ann}(M) = A$ . This means that  $M = (0)$ .

On the other hand, if  $M$  is arbitrary, then  $M = \text{colim}_{\alpha} N_{\alpha}$  with each  $N_{\alpha} \subset M$  finitely generated. But then  $M_{\mathfrak{a}} = \text{colim}_{\alpha} (N_{\alpha})_{\mathfrak{a}}$  because localization is exact. Since each  $N_{\alpha} = (0)$ , it follows that  $\text{colim}_{\alpha} N_{\alpha} = 0$  as well.  $\square$

**Corollary 3.2.2.** *If we have a sequence of modules*

$$\eta : M \xrightarrow{f} T \xrightarrow{g} N,$$

*then  $\eta$  is exact at  $T \iff \eta_{\mathfrak{p}}$  is exact at  $T_{\mathfrak{p}}$  for each  $\mathfrak{p} \in \text{Spec}(A) \iff \eta_{\mathfrak{a}}$  is exact at  $T_{\mathfrak{a}}$  for each  $\mathfrak{a} \in \text{Max}(A)$*

*Proof.* All of the forward directions are clear. Conversely, if  $\eta_{\mathfrak{a}}$  is for every  $\mathfrak{a}$ , then  $M_{\mathfrak{a}} \xrightarrow{f_{\mathfrak{a}}} T_{\mathfrak{a}} \xrightarrow{g_{\mathfrak{a}}} N_{\mathfrak{a}}$  is exact. If  $H = \ker g / \text{im } f$ , then  $H_{\mathfrak{a}} = \ker g_{\mathfrak{a}} / \text{im } f_{\mathfrak{a}} = 0$ . Thus,  $\text{supp}(H) \cap \text{Max}(A) = \emptyset$ , so that  $H = 0$ .  $\square$

**Definition 3.2.3.** Suppose that  $\Pi$  is a property of  $A$ -modules or of morphisms of  $A$ -modules. We say that  $\Pi$  *holds locally for  $A$*  if  $\Pi_{\mathfrak{a}}$  holds for every  $\mathfrak{a} \in \text{Spec}(A)$ .

**Example 3.2.4.**

1.  $M = (0)$  holds locally if and only if it holds globally.
2.  $M \rightarrow T \rightarrow N$  is exact locally if and only if it's exact globally.

**Lemma 3.2.5.** *TFAE.*

- (a)  $M$  is flat over  $A$ .
- (b)  $M$  is locally flat over  $A$ .
- (c)  $M_{\mathfrak{a}}$  is flat over  $A_{\mathfrak{a}}$  for every  $\mathfrak{a} \in \text{Max}(A)$ .
- (d)  $M_{\mathfrak{a}}$  is flat over  $A$  for every  $\mathfrak{a} \in \text{Max}(A)$ .

*Proof.* The fact that (a)  $\implies$  (b)  $\implies$  (c)  $\implies$  (d) is obvious. To see that (c)  $\implies$  (a), suppose that  $M$  is an  $A$ -module such that  $M_{\mathfrak{a}}$  is flat as an  $A_{\mathfrak{a}}$ -module. Suppose that  $0 \rightarrow X \rightarrow Y$  is an exact sequence of  $A$ -modules. Let  $K = \ker(X \otimes_A M \rightarrow Y \otimes_A M)$ . We want to show that  $K = 0$ .

Localizing  $0 \rightarrow K \rightarrow X \otimes_A M \rightarrow Y \otimes_A M$  along  $\mathfrak{a}$  gives an exact sequence  $0 \rightarrow K_{\mathfrak{a}} \rightarrow X_{\mathfrak{a}} \otimes_{A_{\mathfrak{a}}} M_{\mathfrak{a}} \rightarrow Y_{\mathfrak{a}} \otimes_{A_{\mathfrak{a}}} M_{\mathfrak{a}}$ , where we have used the fact that  $(X \otimes_A M)_{\mathfrak{a}} = X \otimes_A M_{\mathfrak{a}} = X_{\mathfrak{a}} \otimes_{A_{\mathfrak{a}}} M_{\mathfrak{a}}$ . But  $M_{\mathfrak{a}}$  is flat over  $A_{\mathfrak{a}}$ . Hence if we tensor the exact sequence  $0 \rightarrow X_{\mathfrak{a}} \rightarrow Y_{\mathfrak{a}}$  with  $M_{\mathfrak{a}}$  over  $A_{\mathfrak{a}}$ , then it will remain exact. This implies that  $\ker(X_{\mathfrak{a}} \otimes_{A_{\mathfrak{a}}} M_{\mathfrak{a}} \rightarrow Y_{\mathfrak{a}} \otimes_{A_{\mathfrak{a}}} M_{\mathfrak{a}}) = 0$ , so that  $K_{\mathfrak{a}} = 0$  for each  $\mathfrak{a}$ . It follows that  $\text{supp}(K) = \emptyset$ , which implies that  $K = (0)$ .  $\square$

**Definition 3.2.6.** If  $A$  is commutative ring, then the *Jacobson radical* of  $A$  is the ideal

$$\text{Jac}(A) \equiv \bigcap_{\mathfrak{a} \in \text{Max}(A)} \mathfrak{a}.$$

**Lemma 3.2.7 (Nakayama).** *If  $A$  is a commutative ring and  $M$  is a finitely generated  $A$ -module with  $\text{Jac}(A) \cdot M = M$ , then  $M = (0)$ .*

*Proof.* Let  $M$  be finitely generated over  $A$ . Choose some finite set of generators  $m_1, \dots, m_t$  of  $M$  of minimal cardinality. If  $M \neq (0)$ , then  $t > 0$ . Then  $m_t \in M = \text{Jac}(A) \cdot M$ . Thus there are  $a_1, \dots, a_t \in \text{Jac}(A)$  such that  $m_t = \sum_{i=1}^t a_i m_i$ . Then

$$(1 - a_t)m_t = \sum_{i=1}^{t-1} a_i m_i.$$

But  $a_t \in \text{Jac}(A)$ , meaning that  $m_t$  belongs to every maximal ideal. Then  $1 - a_t$  cannot be in any maximal ideal. Hence  $1 - a_t$  is a unit in  $A$ . Let  $u \in A$  such that  $u(1 - a_t) = 1$ . Then  $m_t = \sum_{i=1}^{t-1} a_i u m_i$ . This contradicts that  $t$  is minimal.  $\square$

**Corollary 3.2.8 (Classical Nakayama).** *Suppose  $A$  is a local ring with maximal ideal  $\mathfrak{a}_A$ . Let  $M$  be a finitely generated  $A$ -module such that  $\mathfrak{a}_A M = M$ . Then  $M = (0)$ .*

**Proposition 3.2.9.**

1. *If  $A$  is a commutative ring, then the functor  $(-) \otimes^A_{/\text{Jac}(A)} : A\text{-Mod}^{\text{fg}} \rightarrow A/\text{Jac}(A)\text{-Mod}^{\text{fg}}$  is faithful.*
2. *If  $M$  is a finitely generated  $A$ -module and  $m_1, \dots, m_t \in M$  are such that their images  $\bar{m}_1, \dots, \bar{m}_t \in M/\text{Jac}(A) \cdot M$  generate the module  $M/\text{Jac}(A) \cdot M$ , then they generate  $M$ .*

*Proof.* If  $N = \langle m_1, \dots, m_t \rangle \subset M$ , then  $\overline{M/N} = (0)$  since  $\overline{M/N} = \overline{M}/\overline{N}$ . But then  $M \setminus N = 0$  by Lemma 3.2.7.  $\square$

**Proposition 3.2.10.** *If  $A$  is a local ring and  $t$  is the minimal number of generators of a finitely generated  $A$ -module  $M$ , then every generating set for  $M$  contains a generating set of  $t$  elements.*

*Proof.* Let  $m_1, \dots, m_k$  be a generating set for  $M$ . Then  $\bar{m}_1, \dots, \bar{m}_k$  generate  $M/\mathfrak{a}_A M =$  (finite dimensional vector space over  $k_A = A/\mathfrak{a}_A$ ). This must have dimension  $t$  since every spacing subset in  $M/\mathfrak{a}_A M$  lifts to a spanning subset of  $M$ . Choose a linearly independent subset in  $\{\bar{m}_1, \dots, \bar{m}_k\}$  and lift this to  $M$ .  $\square$

**Theorem 3.2.11.** *Let  $A$  be a local ring and  $M$  an  $A$ -module. Assume that one of the following conditions holds.*

(a)  *$A$  is Noetherian with  $M$  finitely generated.*

(b)  *$M$  is finitely presentable.*

*Then  $M$  is free  $\iff M$  is projective  $\iff M$  is flat.*

*Proof.* We only need to show that if  $M$  is flat, then  $M$  is free. Suppose that  $M$  is flat and finitely presentable. We want to show that  $M$  is free. Let  $0 \rightarrow K \rightarrow A^t \rightarrow M \rightarrow 0$  be a finite presentation where  $K$  is finitely generated. Since  $M$  being flat implies that  $(-) \otimes k_A$  is exact, we have that

$$\eta : 0 \rightarrow K \otimes_A k_A \rightarrow k_A^t \rightarrow M \otimes_A k_A \rightarrow 0$$

is exact. Indeed, if  $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$  is a short exact sequence of  $A$ -modules and  $N^n$  is flat, then for every  $A$ -module, the sequence

$$0 \rightarrow N' \otimes M \rightarrow N \otimes M \rightarrow N'' \otimes M \rightarrow 0$$

is exact. To see this, choose a presentation  $0 \rightarrow K \rightarrow F \rightarrow M \rightarrow 0$ , where  $F$  is free. Then we get the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \longrightarrow & N'' & & \\ \downarrow & & \downarrow & & \downarrow & & \\ K \otimes N' & \longrightarrow & K \otimes N & \longrightarrow & K \otimes N'' & & \\ \downarrow \delta_1 & & \downarrow \delta_2 & & \downarrow \delta_3 & & \\ 0 \longrightarrow & F \otimes N' & \longrightarrow & F \otimes N & \longrightarrow & F \otimes N'' & \cdot \\ \downarrow & & \downarrow & & \downarrow & & \\ M \otimes N' & \xrightarrow{\theta} & M \otimes N & \longrightarrow & M \otimes N'' & & \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & 0 & \longrightarrow & 0 & & \end{array}$$

Apply the snake lemma (Lemma 11.2.6 below) to the first two rows.

Returning to  $\eta$ , note that  $k_A^t$  and  $M \otimes_A k_A$  are  $t$ -dimensional vector spaces over  $k_A$ . Hence  $K \otimes_A k_A = 0$ . But  $K$  is a finitely generated  $A$  module. Therefore, Lemma 3.2.7 implies that  $K = 0$ .  $\square$

## 4 Algebraic extensions

### 4.1 Lecture 10

**Definition 4.1.1.** Suppose that  $A \subset B$  where  $A$  and  $B$  are commutative rings.

1. We say that  $u \in B$  is *algebraic over  $A$*  if there is some  $f(x) \in A[x]$  such that  $f(u) = 0$  in  $B$  and  $f \neq 0$ . We say that  $u$  is *transcendental over  $A$*  if it is not algebraic over  $A$ .
2. In general, we say that a collection of elements  $u_1, \dots, u_k \in B$  are *algebraically independent over  $A$*  if there is some  $f(x_1, \dots, x_k) \in A[x_1, \dots, x_k]$  such that  $f \neq 0$  and  $f(u_1, \dots, u_k) = 0$  in  $B$ . We say that  $u_1, \dots, u_k \in B$  are *independent transcendentals over  $A$*  if they are not algebraically independent over  $A$ .
3. We say that  $B \supset A$  is *algebraic* if each  $u \in B$  is algebraic over  $A$ .

Our goal is to understand any algebraic extension of a ring. If  $A$  and  $B$  are domains, then we have a Cartesian diagram

$$\begin{array}{ccc} A & \hookrightarrow & \text{Frac}(A) \\ \downarrow & & \downarrow \\ B & \hookrightarrow & \text{Frac}(B) \end{array}.$$

We have that  $B$  is an algebraic extension of  $A$  if and only if  $\text{Frac}(B)$  is an algebraic extension of  $\text{Frac}(A)$ . This motivates the study of algebraic extensions of fields.

**Definition 4.1.2.** If  $L \supset K$  is a field extension, we say that  $L$  is a *finite extension* if  $L$  is finite dimensional as a vector space over  $K$ . We call  $[L : K] := \dim_K L$  the *degree of the extension*.

*Remark 4.1.3.* Finite field extensions arise naturally from polynomials.

**Definition 4.1.4.** If  $K$  is a field, then  $f(x) \in K[x]$  is called *irreducible* if  $\deg f > 0$  and  $f$  cannot be written as  $f = gh$  where  $g, h \in K[x]$  not units.

**Theorem 4.1.5.** If  $h(x) \in K[x]$  is irreducible, then the ring  $K[x]/(h)$  is a field and the inclusion  $K \subset K[x]/(h)$  is a finite field extension of degree  $\deg h$ .

*Proof.* Recall that  $K[x]$  is a Euclidean domain, in particular, a PID.

**Lemma 4.1.6.** Let  $A$  be a PID and  $u \in A$  be nonzero. TFAE.

- (a)  $A/(u)$  is a field.
- (b)  $(u)$  is prime.
- (c)  $u$  is simple.

*Proof.* The fact that (b) and (c) are equivalent is obvious.

Suppose that  $u$  is not simple, so that  $u = vw$  with  $v, w \in A$  not units. Then in  $A/(u)$  we have two elements  $[v]$  and  $[w]$  such that  $[v] \cdot [w] = [u] = [0]$ . But both  $[v]$  and  $[w]$  are nonzero since  $A$  has cancellations as a PID. Thus,  $A/(u)$  is not a field.

Conversely, if  $u \in A$  is simple, then for any  $x \in A \setminus (u)$  we have that  $(x, u) = (1)$  since  $x$  and  $u$  are coprime. This means that we can find  $a, b \in A$  such that  $ax + bu = 1$ . Then  $[x] \cdot [a] = [1]$ . Hence  $[x]$  is a unit, so that  $A/(u)$  is a field.  $\square$

From this our theorem follows immediately.  $\square$

**Note 4.1.7.**

1. If  $h(x) \in K[x]$  is irreducible and  $L = K[x]/(h)$ , then  $h(x)$  has a natural root in  $L$ , namely,  $t + (h)$ . Moreover, every element in  $L$  can be written in the form  $g(\alpha)$  for some  $g(x) \in K[x]$ .
2. If  $B \supset A$  is a ring extension and  $\alpha_1, \dots, \alpha_k \in B$ , we get an intermediate ring  $A \subset A[\alpha_1, \dots, \alpha_k] \subset B$  where  $A[\alpha_1, \dots, \alpha_k]$  is the image of the evaluation map  $\text{ev}_\alpha : f(x_1, \dots, x_k) \mapsto f(\alpha_1, \dots, \alpha_k)$ . Thus, if  $K$  is a field and  $h(x) \in K[x]$  is irreducible and  $\alpha = t + (h)$ , then  $L := K[x]/(h) = K[\alpha]$ . Observe that  $\alpha$  is algebraic over  $K$ , meaning that  $L$  is generated by a single algebraic element  $\alpha$ .

**Definition 4.1.8.** We say that field extension  $L \supset K$  is *simple* if it is isomorphic to  $K[x]/(h)$  for some irreducible  $h$ .

**Example 4.1.9.**

1.  $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[x]/(x^2 + 1)$ .
2. If  $K$  is any field and  $a \in K$  is not a square, then  $x^2 - a$  is irreducible and we get a simple field extension  $K[\sqrt{a}] := K[t]/(t^2 - a)$ .

Let  $L \supset K$  be any field extension and  $u \in L$  be algebraic over  $K$ . Consider

$$\text{ann}(u) \equiv \{g(x) \in K[x] \mid g(u) = 0\},$$

which is an ideal in  $K[x]$ . Since  $K[x]$  is a PID, we see that this ideal is generated by a single element  $s(x)$ . If we require that  $s(x)$  be monic, then it is uniquely determined. We call this the *minimal polynomial* of  $u$ , denoted by  $\min_u(x)$ .

**Lemma 4.1.10.** *If  $L \supset K$  is a field extension and  $u \in L$  is algebraic over  $K$ , then  $\min_u(x)$  is irreducible and  $K[u]$  is isomorphic to the simple field extension  $K[t]/(\min_u(x))$ .*

*Proof.* If  $\min_u(x) = f(x)g(x)$ , then  $0 = \min_u(u) = f(u)g(u)$ , so that either  $f(u) = 0$  or  $g(u) = 0$ . But  $f, g \mid \min_u$ , so that  $\deg f, \deg g \leq \deg \min_u$ . By the minimality of  $\min_u$ , this implies that  $\deg f = \deg \min_u$  or  $\deg g = \deg \min_u$ . Then either  $\deg f = 0$  or  $\deg g = 0$ .  $\square$



**Theorem 4.1.11.** *Let  $L \supset K$  be a field extension and  $u \in L$ .*

- (a)  *$u$  is algebraic over  $K$  if and only if  $K[u]$  is a finite dimensional vector space over  $K$ .*
- (b) *If  $u$  is algebraic, then  $[K(u) : K] = \deg \min_u$ .*

*Proof.* We have proven (b) in Lemma 4.1.10. For (a), suppose that the ring  $K[u]$  is finite dimensional as a vector space over  $K$ . Then there exist nonnegative integers  $k_1, \dots, k_s$  such that  $k(u) = \text{span}_K(u^{k_1}, \dots, u^{k_s})$ . Thus, if  $m > \max(k_1, \dots, k_s)$ , then  $u^m$  is a  $K$ -linear combination of  $u^{k_1}, \dots, u^{k_s}$ . Write  $u^m = a_1 u^{k_1} + \dots + a_s u^{k_s}$ . Then  $f(x) = x^m - \sum_{i=1}^s a_i x^{k_i}$  satisfies  $f(u) = 0$ . Conversely, if  $u \in L$  is algebraic over  $K$ , then there is some  $n > 0$  such that  $u^n = \text{span}_K(1, u, \dots, u^{n-1})$ . Then  $u^m \in \text{span}_K(1, u, \dots, u^{n-1})$  for any  $m$ . This implies that  $K[u]$  is finite dimensional over  $K$ .  $\square$

**Corollary 4.1.12.** *If  $L \supset K$  is a finite field extension, then  $L$  is algebraic over  $K$ .*

## 4.2 Lecture 11

**Definition 4.2.1.** A finite field extension of  $\mathbb{Q}$  is called a *number field*.

Fix a prime  $p > 0$ . Let  $\epsilon_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ . Then  $\mathbb{Q}(\epsilon_p) \supset \mathbb{Q}$  is a finite extension because  $\epsilon_p$  is annihilated by the polynomial  $x^p - 1$ . It is called the  *$p$ -th cyclotomic field*. Note that  $x^p - 1$  is not minimal since we can factor out  $(x - 1)$ . We claim that  $\frac{x^p - 1}{x - 1}$  is the minimal polynomial, so that  $[\mathbb{Q}(\epsilon_p) : \mathbb{Q}] = p - 1$ . This will hold if we can prove that  $\frac{x^p - 1}{x - 1}$  is irreducible in  $\mathbb{Q}[x]$ .

**Lemma 4.2.2 (Gauss).** *If  $f(x) \in \mathbb{Z}[x]$  is irreducible, then it is irreducible in  $\mathbb{Q}[x]$ .*

*Proof.* Note that if  $p(x) \in \mathbb{Q}[x]$ , then there exists  $N \in \mathbb{Z}_{>0}$  such that  $Np(x) \in \mathbb{Z}[x]$  and the coefficients of  $Np$  are pairwise coprime. Suppose that  $f(x) \in \mathbb{Z}[x]$  is irreducible in  $\mathbb{Z}[x]$ . Suppose, towards a contradiction, that there are  $g(x), h(x) \in \mathbb{Q}[x]$  non-units such that  $f(x) = g(x)h(x)$ . Then  $g(x)$  and  $h(x)$  are  $\mathbb{Q}$ -proportional to some  $\tilde{g}(x)$  and  $\tilde{h}(x)$ , respectively, over  $\mathbb{Z}$  with each having pairwise coprime coefficients. Thus,  $f(x) = \lambda \tilde{g}(x)\tilde{h}(x)$  for some  $\lambda \in \mathbb{Q}^\times$ . Let  $\lambda = \frac{a}{b}$  with  $(a, b) = 1$ . If  $b \neq \pm 1$ , then there is some  $p > 0$  where  $p \mid b$  and  $pf = a\tilde{g}\tilde{h}$ . We have that  $bf, a\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$ . We can reduce mod  $p$  to get  $[bf]_p = [a]_p[\tilde{g}]_p[\tilde{h}]_p$ . But  $f(x) \in \mathbb{Z}[x]$ , so that  $[bf]_p = [b]_p[f]_p = 0$ . Hence  $[a]_p[\tilde{g}]_p[\tilde{h}]_p = 0$  in  $(\mathbb{Z}/p)[x]$ , so that one of  $[a]_p$ ,  $[\tilde{g}]_p$ , and  $[\tilde{h}]_p$  must be 0. But  $(a, b) = 1$ , so that  $[a]_p \neq 0$ . Since each of  $\tilde{g}$  and  $\tilde{h}$  has coprime coefficients, we have that  $[\tilde{g}]_p \neq 0$  and  $[\tilde{h}]_p \neq 0$ , a contradiction.  $\square$

Thus, it suffices to show that  $\frac{x^p - 1}{x - 1}$  is irreducible in  $\mathbb{Z}[x]$ . Let  $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ . Then  $f(x)(x - 1) = x^p - 1$ . By the binomial formula, we see that  $[(x - 1)^p]_p = [x^p - 1]_p$ . Thus,  $[f]_p[x - 1]_p = [(x - 1)^p]_p$ , so that  $[f]_p[(x - 1)]_p = [(x - 1)_p]^p$  and  $[f]_p = [(x - 1)]_p^{p-1}$ . If  $f = gh$  for some non-units  $g$  and  $h$ , then  $[g]_p[h]_p = [(x - 1)]_p^{p-1}$ , which implies that  $[g]_p = [(x - 1)]_p^r$  and  $[h]_p = [(x - 1)]_p^s$  for some  $r$  and  $s$ . Thus,  $[g(1)]_p = [g]_p(1) = 0 = [h]_p(1) = [h(1)]_p$ , meaning that  $p \mid g(1)$  and  $p \mid h(1)$ . Since  $f = gh$ , it follows that  $p^2 \mid f(1) = p$ , a contradiction.

**Theorem 4.2.3.** *Suppose that  $M \supset L \supset K$  is a chain of finite field extensions. Then  $M \supset K$  is also finite with  $[M : K] = [M : L][L : K]$ .*

*Proof.* Let  $e_1, \dots, e_n$  be a basis of  $L$  over  $K$  and  $f_1, \dots, f_m$  be a basis of  $M$  over  $K$ . Then  $\{e_i \cdot f_j\}_{i,j}$  forms a basis of  $M$  over  $K$ .  $\square$

**Note 4.2.4.** Suppose that  $L \supset K$  is a field extension with  $u_1, \dots, u_n \in L$ . We get a ring  $K[u_1, \dots, u_n] = \text{im } \text{ev}_u$ , which is a domain since it's contained in  $L$ . Let  $K(u_1, \dots, u_n) := \text{Frac}(K[u_1, \dots, u_n])$ . Then we have that  $K \subset K[u_1, \dots, u_n] \subset K(u_1, \dots, u_n) \subset L$ . Note that if  $u \in L$  is algebraic over  $K$ , then  $K \subset K[u] = K(u) \subset L$ .

**Theorem 4.2.5.** *Suppose that  $L \supset K$  is a field extension and let  $u_1, \dots, u_n \in L$  be algebraic over  $K$ . Then  $\dim_K K(u_1, \dots, u_n) < \infty$ . In particular,  $K(u_1, \dots, u_n) \supset K$  is an algebraic extension.*

*Proof.* Note that

$$\begin{aligned} K &\subset K(u_1) \subset K(u_1, u_2) \subset \dots \subset K(u_1, \dots, u_n) \\ K(u_1, \dots, u_k) &= K(u_1, \dots, u_{k-1})(u_k). \end{aligned}$$

Since each  $u_k$  is algebraic over  $K$ , we see that  $u_k$  is algebraic over any field containing  $K$ . Thus,  $u_k$  is algebraic over  $K(u_1, \dots, u_{k-1})$ . Hence  $\dim_{K(u_1, \dots, u_{k-1})} K(u_1, \dots, u_k) < \infty$ . By Theorem 4.2.3,  $\dim_K K(u_1, \dots, u_n) < \infty$ .  $\square$

**Definition 4.2.6.**

1. A field  $K$  is *algebraically closed* if for every  $L \supset K$  and every  $u \in L$  algebraic over  $K$ , we have that  $u \in K$ .
2. We say that  $K \subset L$  is *algebraically closed in  $L$*  if any  $u \in L$  that is algebraic over  $K$  belongs to  $K$ .

**Theorem 4.2.7.** *If  $L \supset K$  is a field extension, then*

$$\overline{K} := \{u \in L \mid u \text{ is algebraic over } K\}$$

*is a field that is algebraically closed in  $L$ .*

*Proof.* Let  $u, v \in \overline{K}$ . Then both are algebraic over  $K$ . If  $K \subset K(u, v) \subset L$ , then Theorem 4.2.5 shows that  $K(u, v) \supset K$  is an algebraic extension. Since  $K(u, v) \subset \overline{K}$ , it follows that  $\overline{K}$  is a field.  $\square$

Suppose  $u \in L$  is algebraic over  $\overline{K}$ . Then we can find  $f(x) = \sum_{i=1}^n a_i x^i \in \overline{K}[x]$  such that  $\deg f > 0$  and  $f(u) = 0$ . Hence  $f \in K(a_1, \dots, a_n)[x]$ , so that  $u$  is algebraic over  $K(a_1, \dots, a_n)$ . Hence  $K(a_1, \dots, a_n, u)$  is finite dimensional over  $K(a_1, \dots, a_n)$ . But  $a_1, \dots, a_n \in K$  are algebraic over  $K$ , so that  $K(a_1, \dots, a_n)$  is algebraic over  $K$ . This means that  $u$  is algebraic over  $K$ .

Let  $h$  is an irreducible polynomial over  $K$ . Write  $\tilde{K} = K[x]_{(h)}$  and let  $\alpha$  denote the marked root  $x + (h)$  of  $h$  viewed as a polynomial in  $\tilde{K}[t]$ .

**Lemma 4.2.8 (Main lemma of Galois theory).** *For any  $\varphi : K \rightarrow F$  field homomorphism, the natural map*

$$\left\{ \psi : \tilde{K} \rightarrow F \mid \psi \upharpoonright_K = \varphi \right\} \rightarrow (\text{distinct roots of } h^\varphi \in F[x])$$

*given by  $\psi \mapsto \psi(\alpha)$  is a bijection, where  $h^\varphi$  denotes the polynomial obtained by applying  $\varphi$  to the coefficients of  $h$ .*

*Proof.* Let  $\psi : \tilde{K} \rightarrow F$  be a homomorphism with  $\psi \upharpoonright_K = \varphi$ . Then

$$\begin{aligned} h^\varphi(\psi(\alpha)) &= \varphi(a_n)\psi(\alpha)^n + \varphi(a_{n-1})\psi(\alpha)^{n-1} + \cdots + \varphi(a_1)\psi(\alpha) + \varphi(a_0) \\ &= \psi(a_n)\psi(\alpha)^n + \psi(a_{n-1})\psi(\alpha)^{n-1} + \cdots + \psi(a_1)\psi(\alpha) + \psi(a_0) = \psi(h(\alpha)) \\ &= 0. \end{aligned}$$

Now, let  $\xi \in F$  be a root of  $h^\varphi$ . Define a homomorphism  $K[x] \rightarrow F$  by  $f(x) \mapsto f^\varphi(\xi)$ . Then  $h(x) \mapsto h^\varphi(\xi) = 0$ . Thus, this homomorphism descends to a homomorphism  $\psi : K[x]_{(h)} \rightarrow F$  such that  $\psi(\alpha) = \xi$ . This implies that the assignment  $\psi \mapsto \psi(\alpha)$  is surjective.

Finally, suppose that  $\tilde{\varphi} : \tilde{K} \rightarrow F$  is any homomorphism such that  $\tilde{\varphi} \upharpoonright_K = \varphi$ . Then  $\tilde{\varphi}(\alpha)$  is a root of  $h^\varphi$ . Let  $\psi_{\tilde{\varphi}(\alpha)} : \tilde{K} \rightarrow F$  be the extension that we constructed. Then  $\tilde{\varphi} \upharpoonright_K = \varphi$ , and  $\psi_{\tilde{\varphi}(\alpha)} \upharpoonright_K = \varphi$ . Also, we have that  $\tilde{\varphi}(\alpha) = \xi$  and  $\psi_{\tilde{\varphi}(\alpha)}(\alpha) = \xi$ . This shows that  $\tilde{\varphi} \upharpoonright_{K(\alpha)} = \psi_{\tilde{\varphi}(\alpha)} \upharpoonright_{K(\alpha)}$ . But  $K(\alpha) = \tilde{K}$ .  $\square$

## 5 Splitting fields

### 5.1 Lecture 12

**Definition 5.1.1.** If  $K$  is a field and  $f(x) \in K[x]$ , then a field extension  $L \supset K$  is a *splitting field* for  $f$  if

- (a)  $f(x) = a \prod_{i=1}^n (x - c_i)$  with  $a, c_i \in L$  and
- (b)  $L = K(c_1, \dots, c_n)$ .

**Theorem 5.1.2.** *For every  $f(x) \in K[x]$ , a splitting field for  $f$  exists and is unique up to an isomorphism over  $K$ .*

*Proof.* Consider the tower of fields  $K = K_0 \subset K_1 \subset K_2 \subset \cdots$  where  $K_i = K_{i-1}[\alpha_i]$  and  $\alpha_i$  is a root of an irreducible factor  $f_i$  of  $f$  over  $K_{i-1}$  with  $\deg f_i > 0$ . The degree of  $f$  is fixed, but the number of irreducible factors of  $f$  strictly increases after each step. Hence this sequence of fields will stabilize at some  $K_s$ , which is thus a splitting field for  $f$ .

To prove uniqueness, suppose that  $L \supset K$  is another splitting field for  $f$ . We have  $\varphi_0 : K_0 = K \hookrightarrow L$ . By Lemma 4.2.8, we can extend  $\varphi_0$  to a homomorphism  $\varphi_1 : K_1 \rightarrow L$  provided that  $f_1^{\varphi_0}$  has a root in  $L$ . But by assumption,  $f^{\varphi_0}$  has each of its roots in  $L$ . Since  $f_1 \mid f$ , it follows that  $f_1^{\varphi_0}$  has each of its roots in  $L$  as well. This implies that  $\varphi_1 : K_1 \rightarrow L$  will extend to a map provided that  $\varphi_2 : K_2 \rightarrow L$   $f_2^{\varphi_1} = f_2^{\varphi_0}$  has some root in  $L$ . But this holds since  $f_2 \mid f$ . Continuing in this way, we

get  $\varphi_s : K_s \rightarrow L$  such that  $f_1^{\varphi_s^{-1}}$  has all of its roots in  $L$ . Thus,  $f^{\varphi_s} = f^{\varphi_0}$  has all of its roots in  $L$ . But  $\varphi_s \upharpoonright_K = \varphi_0$ , so that  $\varphi_s$  is injective. But  $L = K(\text{all roots of } f)$ . By construction, all roots of  $f$  belong to  $\text{im } \varphi_s$ . Also,  $K \subset \text{im } \varphi_s$ . Hence  $\varphi_s$  is surjective and thus an isomorphism.  $\square$

**Exercise 5.1.3.** Describe all splitting fields of polynomials of degree 2.

**Example 5.1.4.** Suppose that  $K$  is a field of characteristic  $\neq 2$ . Let  $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ . Let  $L$  be a splitting field for  $f$ . What can  $L$  be? This depends on the splitting behavior of  $f$  over  $K$

- (A) Suppose that  $f$  has all of its roots in  $K$ . Then  $L = K$ , and  $[L : K] = 1$ .
- (B) Suppose that  $f$  has exactly one root in  $K$ . Then  $f(x) = (x - \alpha)g(x)$  with  $\alpha \in K$  and  $g(x)$  a quadratic irreducible in  $K[x]$ . Consider  $L = K[x]_{(g)}$ . Then  $[L : K] = 2$ , and  $g$  has a root in  $L$ . This implies that  $g$  has all of its roots in  $L$ . Hence  $L$  is the splitting field for  $f$ .
- (C) Suppose that  $f$  has no roots in  $K$ . Then  $f$  is irreducible in  $K[x]$ . Let  $K_1 = K[x]_{(f)}$ , which is a simple extension of degree 3. Note that  $f$  has a root  $\alpha_1$  in  $K_1$ . Thus,  $K_1 = K[\alpha_1]$ . Consider  $f(x) = (x - \alpha_1)g(x)$  with  $g \in K_1[x]$  and  $\deg g = 2$ . There are two sub-cases to consider.
  - (a) Suppose that  $g$  has two roots in  $K_1$ . Then  $L = K_1$ , so that  $[L : K] = 3$ .
  - (b) Suppose that  $f$  is irreducible in  $K_1$ . Then  $L = K_2 = K_1[x]_{(g)}$ , so that  $[L : K] = 6$ .

We conclude that if  $L$  is the splitting field for  $f$ , then  $[L : K] \in \{1, 2, 3, 5\}$ .

How can we compute  $[L : K]$  from the coefficients of  $f$ ? We have that  $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$  in  $L[x]$ . Look at  $\text{Discr}(f) := (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \in L$ . This is a symmetric function in  $\alpha_1, \alpha_2, \alpha_3$ . Hence it is expressible in terms of  $a_2, a_1, a_0$ . Note that

$$\text{Discr}(f) = a_1^2a_2^2 - 4a_2^2a_0 - 4a_1^3 + 18a_0a_1a_2 - 27a_0^2.$$

**Proposition 5.1.5.** Suppose that  $f$  has no roots in  $K$ . Then  $[L : K] = 3 \iff \text{Discr } f \in K^2$ .

*Proof.* We know that  $f$  is irreducible over  $K$ . Hence  $K_1 = K[x]_{(f)}$  is an extension of degree 3 in which  $f$  has a root  $\alpha_1$ . Note that  $\text{Discr}(f) \notin K^2 \iff \text{Discr}(f) \notin K_1^2$ . The  $(\implies)$  direction is obvious. For the reverse direction, suppose, towards a contradiction, that  $\text{Discr}(f) \notin K^2$  but  $\text{Discr}(f) \in K_1^2$ . This means that  $[K[\sqrt{\text{Discr}(f)}] : K] = 2$  and  $K \subset K[\sqrt{\text{Discr}(f)}] \subset K_1$ . Thus,  $3 = [K_1 : K] = [K[\sqrt{\text{Discr}(f)}] : K] \cdot [K_1 : K[\sqrt{\text{Discr}(f)}]] = 2 \cdot 1$ , a contradiction.

Now,  $\text{Discr}(f) \in K_1^2 \iff (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in K_1$ . This implies that  $\alpha_2 - \alpha_3 \in K_1$ . Indeed,  $f \in K_1[x]$  satisfies  $f(x) = (x - \alpha_1)g(x)$ , and  $\alpha_2, \alpha_3 \in L$  are roots of  $g$ . Therefore, we have in  $L$  that  $g(\alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \in L$ . But  $g \in K_1[x]$  and  $\alpha_1 \in K_1$ , so that  $g(\alpha_1) \in K_1$ . It follows that  $\alpha_2 - \alpha_3 \in K_1$ . Hence  $\text{Discr}(f) \in K_1^2 \iff \alpha_2 - \alpha_1 \in K_1$ . But  $-\alpha_2 - \alpha_3$  is a coefficient of  $g$  in  $K_1$ . Therefore,  $\alpha_2, \alpha_3 \in K_1$ .  $\square$

**Note 5.1.6.**

1. Suppose that  $K$  is a finite field. Then  $\text{char } K > 0$ .
2. Suppose that  $K$  is any field such that  $\text{char } K = p > 0$ . Then the natural map  $\varphi : K \rightarrow K$  given by  $x \mapsto x^p$  respects addition due to the binomial theorem. Hence it is a field homomorphism, called the *Frobenius morphism*. If  $K$  is finite, then this map is an automorphism. In general,  $\text{im } \varphi = K^p \subset K$  is a subfield.
3. If  $K$  has characteristic  $p$ , then the natural map  $\mathbb{F}_p \rightarrow K$  given by  $[n] \mapsto \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$  is a field extension. Therefore, if  $K$  is finite, then  $K \supset \mathbb{F}_p$  is a finite field extension. In this case, if  $K$  has degree  $n$ , then  $K \cong \mathbb{F}_p^{\oplus n}$  is a vector space over  $\mathbb{F}_p$ . Hence  $|K| = |\mathbb{F}_p|^n = p^n$ .

## 6 Finite fields

**Theorem 6.0.1.** *For every prime  $p$  and integer  $n > 0$ , there is some finite field  $K$  consisting of  $p^n$  elements that is unique up to an isomorphism over  $\mathbb{F}_p$ .*

*Proof.* We first prove uniqueness. If  $F$  is a finite field with  $q := p^n$  elements, then  $|F^\times| = q - 1$ . It follows that for any  $a \in F^\times$ ,  $a^{q-1} = 1$ . But then for any  $a \in F$ ,  $a^q = a$ , so that each element of  $F$  is a root of  $x^q - x \in \mathbb{F}_p[x]$ . Then  $\prod_{a \in F} (x - a) \mid x^q - x$  in  $F[x]$ . This implies that  $x^q - x = \prod_{a \in F} (x - a)$  in  $F[x]$ . This means that  $F$  is a splitting field for  $x^q - x$  over  $\mathbb{F}_p$ , which must be unique up to isomorphism.

To prove existence, consider  $F$  the splitting field for  $x^q - x$  over  $\mathbb{F}_p$ . We want to show that  $|F| = q$ .

**Note 6.0.2.** If  $A$  is any commutative ring, then  $A[x]$  has a natural derivation. There exists a unique map  $\frac{d}{dx} : A[x] \rightarrow A[x]$  such that  $\frac{d}{dx}(a) = 0$  for any  $a \in A$ ,  $\frac{d}{dx}(x) = 1$ , and  $\frac{d}{dx}$  satisfies the Leibniz rule, i.e.,  $\frac{d}{dx}(fg) = \frac{df}{dx}g + f\frac{dg}{dx}$ . Note that  $\frac{d}{dx}$  is given by  $\frac{d}{dx}(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0) = na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \cdots + 0$ . Then  $\frac{d}{dx}$  is an  $A$ -module homomorphism. If  $A \subset B$  is a subring, then we get compatible derivations  $\frac{d}{dx} \hookrightarrow A[x] \subset B[x] \hookleftarrow \frac{d}{dx}$ .

Returning to our proof, consider  $f(x) = x^q - x$ . Then since  $F \supset \mathbb{F}_p$  is the splitting field for  $f(x)$ , it follows that  $f(x) = \prod_{i=1}^q (x - c_i)$  where  $c_i \in F$ . How many distinct roots does  $f(x)$  have in  $F$ ? If  $f(x)$  has a repeated root, then we can write  $f(x) = (x - c)^2 g(x)$  in  $F[x]$ . This implies that  $\frac{df}{dx}(x) = 2(x - c)g + (x - c)^2 \frac{dg}{dx}$  will also have  $c$  as a root. But  $\frac{df}{dx} = qx^{q-1} - 1 = -1$  in  $\mathbb{F}_p[x] \subset F[x]$ . But in this case  $\frac{df}{dx}$  has no roots. Thus,  $f(x)$  has no repeated roots in  $F$ , so that  $|F| \geq q$ .

Now consider  $R_f := \{c \in F \mid f(c) = 0\}$ . Note that  $\mathbb{F}_p \subset R_f \subset F$  and that  $R_f = \{c \in F \mid \varphi^n(c) = c\}$  where  $\varphi$  denotes the Frobenius map. But since  $\varphi$  is a field automorphism of  $F$ , so is  $\varphi^n$ . Hence the fixed points of  $\varphi^n$  form a subfield. This means that  $R_f$  is a subfield, hence a splitting field for  $f$ . Thus,  $R_f \cong F$ .  $\square$

### 6.1 Lecture 13

We write  $\mathbb{F}_q$  for the splitting field for  $x^q - x \in \mathbb{F}_p[x]$ .

**Proposition 6.1.1.** *The group  $\mathbb{F}_q^\times$  is a cyclic group of order  $q - 1$ .*

*Proof.* By the structure theorem for finite abelian groups, we get

$$\begin{aligned} \mathbb{F}_q^\times \cong \mathbb{Z}/p_1^{m_{11}} \times \mathbb{Z}/p_1^{m_{12}} \times \cdots \times \mathbb{Z}/p_1^{m_{1k}} \times \mathbb{Z}/p_2^{m_{21}} \times \mathbb{Z}/p_2^{m_{22}} \times \cdots \\ \times \mathbb{Z}/p_2^{m_{2k}} \times \cdots \times \mathbb{Z}/p_s^{m_{s1}} \times \mathbb{Z}/p_s^{m_{s2}} \times \cdots \times \mathbb{Z}/p_s^{m_{sk}}. \end{aligned}$$

Let  $\alpha_i = p_1^{m_{1i}} p_2^{m_{2i}} \cdots p_s^{m_{si}}$  for each  $i = 1, \dots, k$ . Hence  $|\mathbb{F}_q^\times| \mid d_1 d_2 \cdots d_k$  where  $d_1 \mid d_2 \mid \cdots \mid d_k$ . Hence every element in  $\mathbb{F}_q^\times$  has order dividing  $d_k$ . For any  $a \in \mathbb{F}_q$ ,  $a^{d_k+1} = a$ , so that  $|\mathbb{F}_q| = \deg x^{d_k+1} - x = d_k + 1$ . Then  $q \leq d_k + 1$ , so that  $q - 1 \leq d_k$ . Since  $d_k \mid q - 1$ , we have that  $d_k = q - 1$ , and thus  $d_1 = d_2 = \cdots = d_{k-1} = 1$ . Hence

$$\mathbb{F}_q^\times \cong \mathbb{Z}/p_1^{m_{1k}} \times \mathbb{Z}/p_2^{m_{2k}} \times \cdots \times \mathbb{Z}/p_s^{m_{sk}}.$$

Since the  $p_i^{m_{ik}}$  are pairwise coprime, it follows that  $\mathbb{F}_q^\times \cong \mathbb{Z}/p_1^{m_{1k}} p_2^{m_{2k}} \cdots p_s^{m_{sk}}$ . □

**Corollary 6.1.2.**  $\mathbb{F}_q = \mathbb{F}_p(\sigma)$ .

*Proof.* Since  $\mathbb{F}_q^\times$  is cyclic, we know that  $\mathbb{F}_q^\times = \langle \sigma \rangle$ . □

**Proposition 6.1.3.**  *$\text{Aut}(\mathbb{F}_q)$  is a cyclic group of order  $n$ . In fact,  $\text{Aut}(\mathbb{F}_q) \cong \langle \varphi \rangle$  where  $\varphi$  denotes the Frobenius map.*

*Proof.* We have arranged it so that  $\mathbb{F}_q$  is unique up to isomorphism over  $\mathbb{F}_p$ , so that each  $\psi \in \text{Aut}(\mathbb{F}_q)$  restricts to the identity on  $\mathbb{F}_p \subset \mathbb{F}_q$ . This implies that  $\text{Aut}(\mathbb{F}_q) \cong \text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ , which is the subgroup of all  $\psi : \mathbb{F}_q \xrightarrow{\cong} \mathbb{F}_q$  such that  $\psi|_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$ .

**Lemma 6.1.4.** *Let  $L \supset K$  be a finite field extension of degree  $n$ . Then we have that  $|\text{Aut}(L/K)| \leq n$ .*

*Proof.* Since  $[L : K] = n < \infty$ , we can construct  $L$  as a tower  $K = K_0 \subset K_1 \subset \cdots \subset K_s = L$  where  $K_{i+1} = K_i[\alpha_i]$  and  $\alpha_i$  is a root of an irreducible  $f_i(x) \in K_i[x]$ . Consider  $\varphi_0 : K \hookrightarrow L$  the natural inclusion. Applying Lemma 4.2.8, we see that  $\varphi_0$  extends to  $\varphi_1 : K_1 \rightarrow L$  in finitely many ways such that the number of such  $\varphi_1$ 's equals the number of distinct roots of  $f_0^{\varphi_0}$  in  $L$ . This quantity is  $\leq \deg f_0 = [K_1 : K_0]$ . Each  $\varphi_1$  extends to a map  $\varphi_2 : K_2 \rightarrow L$  in at most  $\deg f_1 = [K_2 : K_1]$  ways. Therefore,  $\varphi_0$  will extend to a map  $\varphi_s : L \rightarrow L$  in  $[K_1 : K_0][K_2 : K_1] \cdots [K_s : K_{s-1}]$  many ways. It follows that

$$|\text{Aut}(L/K)| \leq \prod_{i=0}^{s-1} [K_{i+1} : K_i] = [L : K] = n.$$

□

**Corollary 6.1.5.** *If  $f(x) \in K[x]$  and  $L$  is a splitting field for  $f$  and  $f$  has distinct roots in  $L$ , then  $|\text{Aut}(L/K)| = [L : K]$ .*

We have that  $|\text{Aut}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p] = n$ . If  $\varphi \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ , then  $\varphi^n = \text{id}$ . Thus, it suffices to show that  $\varphi^m \neq \text{id}$  for any  $m < n$ . Suppose that  $m$  has  $\varphi^m = \text{id}$ . Then  $\varphi^m(a) = a$  for every  $a \in \mathbb{F}_q$ . Therefore,  $q^{p^m} = a$  for each  $a \in \mathbb{F}_q$ , so that  $p^n = q = |\mathbb{F}_q| \leq p^m$ . Then  $m \geq n$ .

This completes our main proof. □

**Proposition 6.1.6.** *There is a bijection (subfields of  $\mathbb{F}_q$ )  $\cong_{\text{Set}}$  (subgroups of  $\text{Aut}(\mathbb{F}_q)$ ).*

*Proof.* Let  $F \subset \mathbb{F}_q$  be a subfield, so that  $\mathbb{F}_p \subset F \subset \mathbb{F}_q$ . We have that  $|F| \mid |\mathbb{F}_q| = p^n$ , so that  $|F| \leq p^d$  for some  $d \leq n$ . Since  $\mathbb{F}_q \supset F$ , we have that  $\mathbb{F}_q$  is a vector space over  $F$ . If  $[\mathbb{F}_q : F] = r$ , then  $\mathbb{F}_q \cong F^{\oplus r}$  as  $F$ -vector spaces. Note that

$$p^n = |\mathbb{F}_q| = |F|^r = (p^d)^r = p^{dr},$$

which implies that  $d \mid n$ .

Since  $F$  is a finite field, it follows that  $F^\times$  is cyclic of order  $p^d - 1$ . Hence any  $a \in F \subset \mathbb{F}_q$  satisfies  $a^{p^d} = a$ . But if  $d \mid n$ , then  $x^q - x = x^{p^n} - x = (x^{p^d} - x)g(x)$  because  $p^n - 1 = p^{dr} - 1 = (p^d)^r - 1 = (p^d - 1)m$  so that  $x^{q-1} - 1 = (x^{p^d-1} - 1)g(x)$ . But  $\mathbb{F}_q$  is the splitting field for  $x^q - x$ , and all roots of this are distinct. Thus, there are exactly  $p^d$  roots of  $x^q - x$  that are the distinct roots of  $x^{p^d} - x$ . Therefore,

$$F = \mathbb{F}_{p^d} = \left( \text{subfield of } \mathbb{F}_q \text{ that is the splitting field for } x^{p^d} - x \right) = \left( \text{fixed subfield of } \varphi^d \right).$$

Hence  $F$  is the fixed point subgroup of  $\langle \varphi^d \rangle \trianglelefteq \text{Aut}(\mathbb{F}_q)$ .

Let  $\psi \in \text{Aut}(\mathbb{F}_q)$  with  $\psi \notin \langle \varphi^d \rangle$ . Then  $\psi = \varphi^e$  for some  $e \geq 0$  such that  $d \nmid e$ . If  $\xi$  generates  $F^\times$  and  $\xi^{p^e} = \psi(\xi) = \xi$ , then  $p^d - 1 \mid p^e - 1$  since  $|F^\times| = p^d - 1$ . But this is impossible, which implies that  $\psi \upharpoonright_F \neq \text{id}_F$ . Therefore,  $\langle \varphi^d \rangle = \text{Aut}(\mathbb{F}_q/F)$ , and we have a bijection

$$(\text{subfields of } \mathbb{F}_q) \cong_{\text{Set}} (\text{subgroups of } \text{Aut}(\mathbb{F}_q))$$

$$F \mapsto \text{Aut}(\mathbb{F}_q/F)$$

$$\mathbb{F}_q^G \leftrightarrow G.$$

□

## 6.2 Lecture 14

**Proposition 6.2.1.**

1. Let  $\mathbb{F}_q^\times = \langle \theta \rangle$ . Then  $\mathbb{F}_q = \mathbb{F}_p(\theta)$ , meaning that  $\theta$  is a primitive element for the extension  $\mathbb{F}_q \supset \mathbb{F}_p$ . Further, if  $h$  denotes the minimal polynomial of  $\theta$  over  $\mathbb{F}_p$ , then  $\mathbb{F}_q$  is the splitting field for  $h$ .

*Proof.* Every nonzero element of  $\mathbb{F}_q$  is a power of  $\theta$ . Hence  $\mathbb{F}_q = \mathbb{F}_p(\theta)$ . Now, note that  $\deg h = n$  because  $[\mathbb{F}_q : \mathbb{F}_p] = n$ . Write  $h(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  where each  $a_i \in \mathbb{F}_p$ . If we view  $h$  over  $\mathbb{F}_q$ , then  $\varphi(a_i) = a_i$  due to Fermat's little theorem. Hence  $\varphi(h(x)) = h(\varphi(x))$  for any  $x \in \mathbb{F}_q$ , meaning that  $\varphi(c)$  is a root of  $h$  whenever  $c$  is a root. Thus, we get  $n$  roots of  $h$ .

$$\theta, \theta^p, \theta^{p^2}, \dots, \theta^{p^{n-1}}$$

If  $K$  is the splitting field for  $h$ , then  $\mathbb{F}_p \subset K \subset \mathbb{F}_q$ . But  $[K : \mathbb{F}_p] = n = [\mathbb{F}_q : \mathbb{F}_p]$ , so that  $K = \mathbb{F}_q$ . □

2. Let  $m \geq 0$  be any integer and  $q = p^n$ . Then there is some irreducible polynomial over  $\mathbb{F}_q$  of degree  $m$

*Proof.* Let  $\mathbb{F}_{p^{mn}}^\times = \langle \theta \rangle$ . Then the minimal polynomial  $p(x)$  of  $\theta$  over  $\mathbb{F}_q$  has degree  $m$ , and  $p(x)$  is irreducible since it is minimal.  $\square$

## 7 Cyclotomic fields

Let  $q = p^n$  and  $d > 0$  be any integer. Among the finitely many polynomials over  $\mathbb{F}_q$  of degree  $d$ , how many of these are irreducible? We have just shown that at least one is irreducible.

**Definition 7.0.1.** Define the *Möbius function*  $\mu : \mathbb{Z}_{>0} \rightarrow \{-1, 0, 1\}$  by

$$n \mapsto \begin{cases} -1 & n = 1 \\ (-1)^k & n = p_1 \cdots p_k \text{ where the } p_i \text{ are pairwise distinct} \\ 0 & n \text{ is divisible by a square} \end{cases}$$

**Proposition 7.0.2.**

1.  $\mu(k) \neq 0$  for some  $k$ .
2.  $\mu(nm) = \mu(n)\mu(m)$  when  $(n, m) = 1$ .
3.  $\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}$ . (This completely characterizes the Möbius function.)

*Proof.* Let  $n > 0$  be an integer and write  $p_1^{k_1} \cdots p_k^{r_k}$  where the prime  $p_i$  are pairwise distinct. Let  $n_0 = p_1 \cdots p_k$ . Then  $\sum_{d|n} \mu(d) = \sum_{d|n_0} \mu(d)$ . If  $d | n_0$ , then  $d = p_{i_1} \cdots p_{i_s}$ , so that  $\mu(d) = (-1)^s$ . By the binomial theorem, it follows that

$$\begin{aligned} \sum_{d|n_0} \mu(d) &= \sum_{s=0}^k \binom{k}{s} (-1)^s \\ &= (1-1)^k = \begin{cases} 1 & k = 0 \\ 0 & k > 0 \end{cases}. \end{aligned}$$

$$\text{Thus, } \sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}.$$

$\square$

**Corollary 7.0.3.** For any  $m \in \mathbb{Z}_{>0}$  and  $d | m$ , we have that

$$\sum_{d|n|m} \mu\left(\frac{m}{d}\right) = \begin{cases} 1 & d = m \\ 0 & d \neq m \end{cases}.$$



**Lemma 7.0.4.** *Let  $A$  be an abelian group and  $f, g : \mathbb{Z}_{>0} \rightarrow A$  be functions such that  $f(n) = \sum_{d|n} g(d)$  for every  $n$ . Then we obtain the so-called Möbius inversion formula*

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d). \quad (\dagger)$$

If  $A$  is written multiplicatively, then this becomes

$$g(n) = \prod_{d|n} f(d)^{\mu\left(\frac{n}{d}\right)}.$$

*Proof.* We compute

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k|d} g(k) \\ &= \sum_{d|n} \sum_{k|d} \mu\left(\frac{n}{d}\right) g(k) \\ &= \sum_{k|n} g(k) \sum_{d: k|d|n} \mu\left(\frac{n}{d}\right) \\ &= \sum_{k|n} g(k) \delta(k, n) \\ &= g(n). \end{aligned}$$

□

**Definition 7.0.5.** Define the *Euler (totient) function*  $\varphi : \mathbb{Z}_{>0} \rightarrow \mathbb{Z}$  by

$$\varphi(n) = \# \{m \in \mathbb{Z}_{>0} : m \leq n, (m, n) = 1\}.$$

If  $n \in \mathbb{Z}_{>0}$ , then  $n = \sum_{d|n} \varphi(d)$ . Therefore, if  $f : \mathbb{Z}_{>0} \rightarrow \mathbb{Z}$  is given by  $f(n) = n$  and  $g := \varphi$ , then we can apply  $(\dagger)$  to get

$$\begin{aligned} \varphi(n) = g(n) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) d \\ &= \sum_{m|n} \mu(m) \frac{n}{m} = \left( \sum_{m|n} \frac{\mu(m)}{m} \right) n. \end{aligned}$$

**Lemma 7.0.6.** *If  $n = p_1^{r_1} \cdots p_k^{r_k}$ , then  $\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$ .*

*Proof.* Let  $n_0 = p_1 \cdots p_k$ . Then

$$\begin{aligned}
 \sum_{m|n} \frac{\mu(m)}{m} &= \sum_{m|n_0} \frac{\mu(m)}{m} \\
 &= \underbrace{1}_{m=1} - \sum_{i=1}^k \frac{1}{p_i} \\
 &\quad + \sum_{i < j} \frac{1}{p_i p_j} + \cdots + (-1)^s \sum_{i_1 < \cdots < i_s} \frac{1}{p_{i_1} \cdots p_{i_s}} \\
 &\quad + \cdots + (-1)^k \frac{1}{p_1 \cdots p_k} \\
 &= \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).
 \end{aligned}$$

□

Let  $p(x) = x^n - 1 \in \mathbb{Q}[x]$  with  $n > 0$ . Let  $\Gamma_n$  be the splitting field for  $p(x)$ . We know that  $\Gamma_n = \mathbb{Q}(\zeta_n)$ , where  $\zeta_n$  denotes a primitive  $n$ -th root of unity in  $\mathbb{C}$ . Let the set  $\text{Prim}_n$  consist of all the primitive  $n$ -th roots of unity.

We have that  $\mu_n = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\} = \coprod_{d|n} \text{Prim}_d$ . Define the  $d$ -th cyclotomic polynomial as

$$\Phi_d(x) = \prod_{\alpha \in \text{Prim}_d} (x - \alpha).$$

For example,

$$\begin{aligned}
 \Phi_1 &= x - 1 \\
 \Phi_2 &= x + 1 \\
 \Phi_3 &= x^2 + x + 1 \\
 \Phi_4 &= x^2 + 1 \\
 &\vdots \\
 \Phi_p &= x^{p-1} + x^{p-2} + \cdots + x + 1 \text{ with } p \text{ prime.}
 \end{aligned}$$

Note that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Consider the functions  $\Phi_{(-)} : \mathbb{Z}_{>0} \rightarrow \mathbb{C}(x)^\times$  and  $f : \mathbb{Z}_{>0} \rightarrow \mathbb{C}(x)^\times$  where  $f(n) = x^n - 1$ . We can apply (†) to get

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})},$$

which is a rational function over  $\mathbb{Z}$ . We can write  $\Phi_n(x) = \frac{a(x)}{b(x)}$  with  $b(x)$  monic. Write  $\Phi_n(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_0$  and set  $M = \text{lcm}\{c_i \mid p_i = \frac{t_i}{c_i}, i = 1, \dots, m-1\}$ . Let  $P_i = Mp_i$  for each  $i = 1, \dots, m-1$  and  $P_m = M$ . Since  $M\Phi_n(x)b(x) = Ma(x) \in \mathbb{Z}[x]$ , we see that  $M$  divides

each coefficient of  $M\Phi_n(x)b(x)$ . Suppose, towards a contradiction, that  $M > 1$ . Then there exists a prime divisor  $p$  of  $M$ . By our choice of  $M$ , there exists a maximal  $0 \leq i_0 \leq m$  such that  $p \nmid P_{i_0}$ . If  $\deg b(x) = s$ , then the coefficient of  $X^{m+s}$  in  $M\Phi_n(x)b(x)$  has the form  $M + p \cdot t$  for some  $t \in \mathbb{Z}$ . But this is not divisible by  $p$  and thus not divisible by  $M$ , a contradiction. Thus,  $M = 1$ , so that  $\Phi_n(x) \in \mathbb{Z}[x]$ .

Moreover, since  $\deg \Phi_n = \varphi(n)$ , it follows that  $[\Gamma_n : \mathbb{Q}] = \varphi(n)$ .

## 7.1 Lecture 15

Let  $q = p^n$ . Let  $\psi_d(q) = \#\{p(x) \text{ irreducible over } \mathbb{F}_q \mid \deg p(x) = d\}$ . If  $f(x) \in \mathbb{F}_q[x]$  is irreducible, then  $F = \mathbb{F}_q[x]_{(f)}$  is a finite field. Thus,  $\#F = g^d = p^{nd}$ , so that  $F$  is the splitting field for  $x^{p^{nd}} - x$  over  $\mathbb{F}_p$ . Also,  $F$  is just the set of roots of  $x^{p^{nd}} - x$ . By construction, the polynomial  $f(x) \in \mathbb{F}_q[x]$  has a root over  $F$ , and  $x^{p^{nd}} - x \in \mathbb{F}_q[x]$  has a root in  $F$ .

Since  $f(x)$  is irreducible in  $\mathbb{F}_q[x]$ , we see that  $(f, x^{p^{nd}} - x) \in \{1, f\}$  in  $\mathbb{F}_q[x]$ . But if  $(f, x^{p^{nd}} - x) = 1$ , then  $1 = a(x)f(x) + b(x)(x^{p^{nd}} - x)$ , with  $a, b \in \mathbb{F}_q[x]$ . If we write this as an equation in  $F[x]$ , then evaluating on  $\alpha \in F$  a common root of  $f(x)$  and  $x^{p^{nd}} - x$  will give us a contradiction. Hence  $f(x) \mid x^{p^{nd}} - x$  in  $\mathbb{F}_q[x]$ . Since all roots of  $x^{p^{nd}} - x$  are pairwise distinct, we see that any irreducible monic polynomial of degree  $d$  over  $\mathbb{F}_q$  appears exactly once in the decomposition of  $x^{p^{nd}} - x$  into irreducibles. Note that if  $m = dr$ , then

$$x^{q^d} - x \mid \underbrace{x^{q^m} - x}_{\text{distinct roots}},$$

and thus every irreducible monic polynomial over  $\mathbb{F}_q$  of degree dividing  $m$  appears exactly once in the irreducible decomposition of  $x^{q^m} - x$ .

For each  $d \geq 1$ , let  $f_{d,1}, f_{d,2}, \dots, f_{d,\psi_d(q)}$  be irreducible monic polynomials over  $\mathbb{F}_q$  of degree  $d$ . Then for any  $m \geq 1$ , we get

$$x^{q^m} - x = \prod_{d \mid m} \prod_{k=1}^{\psi_d(q)} f_{d,k}(x),$$

so that  $q^m = \sum_{d \mid m} d\psi_d(q)$ . Then

$$\psi_d(q) = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) q^d.$$

### Example 7.1.1.

$$\begin{aligned} \psi_2(2) &= \frac{1}{2}(2^2 - 2) = 1. \\ \psi_3(2) &= \frac{1}{2}(2^3 - 2) = 2. \end{aligned}$$

*Remark 7.1.2.* A randomly chosen polynomial over  $\mathbb{F}_q$  of degree  $d$  will be irreducible with probability  $\approx \frac{1}{d}$ . Given a polynomial  $p(x)$  over  $\mathbb{F}_q$  of degree  $d$ , there is no known algorithm that is polynomial in  $d$  for deciding whether  $p(x)$  is irreducible.

## 8 Galois theory

**Definition 8.0.1.** If  $L \supset K$  is a field extension, then the *Galois group* is

$$\text{Gal}(L/K) \equiv \{\varphi \in \text{Aut}(L) : \varphi|_K = \text{id}_K\}.$$

**Theorem 8.0.2.** Let  $L \supset K$  be a field extension of degree  $n < \infty$ . Let  $G \leq \text{Gal}(L/K)$ .

- (a)  $L^G = K \iff |G| = n$ .
- (b) If  $L^G = K$  and  $K \subset P \subset Q \subset L$  is a chain of field extensions, then every homomorphism  $\varphi : P \rightarrow L$  over  $K$  extends to a homomorphism  $Q \rightarrow L$  in exactly  $[Q : P]$  many ways.

*Proof.*

- (a) For the ( $\Leftarrow$ ) direction, note that if  $G \leq \text{Aut}(L)$ , then tautologically  $G \leq \text{Gal}(L/L^G)$ . Hence  $|G| \leq |\text{Gal}(L/L^G)| = [L : L^G]$ . If  $G \leq \text{Gal}(L/K)$ , then  $L \subset L^G \subset L$ , so that  $[L : L^G] \leq [L : K] = n$ . This means that  $|G| \leq n$ .

Conversely, let  $L^G = K$ . Take  $\alpha \in L$  and let  $\text{Orb}_G(\alpha) = \{\lambda_1, \dots, \lambda_m\} \subset L$ . Consider

$$f(x) = \prod_{i=1}^m (x - \lambda_i) \in L[x].$$

But the coefficients are symmetric polynomials in  $\lambda_i$ , and any  $g \in G$  permutes the  $\lambda_i$ . In this case,  $g$  permutes the coefficients of  $f(x)$ . Hence  $f(x) \in L^G[x] = K[x]$ . By construction,  $\alpha$  is a root of  $f(x)$ , the minimal polynomial of  $\alpha$ . We can decompose  $f(x)$  into linear factors in  $L$ .

Apply part (b) to  $P = K$  and  $Q = L$ . In this case, (b) implies that if  $L^G = K$ , then  $|\text{Gal}(L/K)| = [L : K] = n$ . Thus, we must show that  $G = \text{Gal}(L/K)$ .

Let  $\varphi \in \text{Gal}(L/K)$ . Recall that  $f(x)$  is the minimal polynomial of  $\alpha$  over  $K$ . Note that  $\varphi(x)$  is a root of  $f^\varphi(x)$ . Indeed, since  $\varphi|_K = \text{id}_K$ , we have that  $f^\varphi(x) = f(x)$ . Hence  $\varphi(\alpha) \in \text{Orb}_G(\alpha)$ , so that there exists  $g \in G$  such that  $\varphi(\alpha) = g(\alpha)$ . If  $L$  is a finite field, then we can take  $\alpha$  to be the generator of  $L^\times$ , in which case  $\varphi(\alpha) = g(\alpha) \implies \varphi(\alpha^k) = g(\alpha^k)$  for each  $k \implies \varphi = g$ . If  $L$  is infinite, then  $K$  is infinite and for any  $g \in G$ , we consider  $L_g = \{a \in L \mid \varphi(a) = g(a)\} \subset L$ . By definition,  $L_g = L^{g^{-1} \circ \varphi}$  is a subfield in  $L$ . This contains  $K$  because  $g^{-1} \circ \varphi \in \text{Gal}(L/K)$ . Therefore,  $K \subset L_g \subset L$  is a field extension, meaning that  $L_g$  is a  $K$ -vector subspace in  $L$ .

We have shown that  $L = \bigcup_{g \in G} L_g$ .

**Claim.** If  $K$  is an infinite field and  $V$  is a finite-dimensional  $K$ -vector space and  $V_1, V_2, \dots, V_g \subset V$  are subspaces, then  $V = \bigcup_{i=1}^g V_i \implies V = V_k$  for some  $k$ .

*Proof.* Suppose that each  $V_i \subsetneq V$  and that  $V = \bigcup_{i=1}^g V_i$ . Then there exists a linear map  $f_i : V \rightarrow K$  such that  $f_i|_{V_i} = 0$  and  $f_i \neq 0$ . Then  $f : V \rightarrow K$  given by  $f = \prod_{i=1}^g f_i$  is the function associates with a nonzero polynomial in  $V = K^n$  of degree  $s$ . But  $f$  is the zero function since  $V = \bigcup_{i=1}^g V_i$ , a contradiction.  $\square$

- (b) Suppose that  $K \subset P \subset L$ . Let  $K \subset P \subset Q \subset L$  where  $Q = P(\alpha) = P[\alpha]$  and  $\alpha$  is a root of some irreducible  $h(x) \in P[x]$ . Let  $f(x) = \prod_{i=1}^m (x - \lambda_i)$  where  $\text{Orb}_G(\alpha) = \{\lambda_1, \dots, \lambda_m\} \subset L$ . Then  $f(x), g(x) \in P[x]$  have a common root, and  $h(x)$  is irreducible. Hence  $h \mid f$  in  $P[x]$ .

Let  $\varphi : P \rightarrow L$  be any field homomorphism over  $K$ . Then  $h^\varphi \mid \underbrace{f^\varphi}_f$  in  $L[x]$ . But  $f$  decomposes into distinct linear factors in  $L[x]$ . Hence  $h^\varphi$  equals a product of a subcollection of these factors. It follows that  $h^\varphi$  has  $\deg h^\varphi = \deg h$  distinct roots in  $L$ . By Lemma 4.2.8, since  $Q \cong P[x]/(h)$ , we see that  $\varphi$  extends in exactly  $\deg h - [Q : P]$  many ways.

This proves our result for simple field extensions. Since every finite extension is a tower of simple extensions, we are done by induction on the length of the tower. □

**Definition 8.0.3.** A finite field extension  $L \supset K$  is a *Galois extension* if  $|\text{Gal}(L/K)| = [L : K]$ .

**Corollary 8.0.4.** If  $L \supset K$  is a Galois extension, then  $K \subset P \subset L \implies L \supset P$  is Galois as well.

*Proof.* Take  $Q = L$  and apply (b) then (a). □

**Definition 8.0.5.** If  $K$  is a field and  $f(x) \in K[x]$ , then we say that  $f$  is *separable over  $K$*  if  $f$  has no repeated roots in any finite extension of  $K$ . Equivalently,  $f$  has no repeated roots in its splitting field.

## 8.1 Lecture 16

**Proposition 8.1.1.** A polynomial  $f(x) \in K[x]$  is separable over  $K$  if and only if  $(f, f') = 1$ .

*Proof.* If  $f, g \in K[x]$ , then  $(f, g) \in K[x]$ . Suppose there exists  $L \supset K$  such that  $f$  has a multiple root in  $L$ . Then there exists an irreducible polynomial  $h(x) \in L[x]$  such that  $h^2 \mid f$ . This implies that  $f = h^2 q$ , so that  $f' = 2hh'q + h^2q' = h(2h'q + hq')$ . Hence  $h \mid f'$  in  $L[x]$ . Then  $h \mid (f, f')$  in  $L[x]$ , making  $(f, f') \neq 1$ .

Conversely, suppose that  $(f, f') \neq 1$ . Then there exists  $h$  irreducible in  $K[x]$  such that  $h \mid f'$  and  $h \mid f$  in  $K[x]$ . We can write  $f = hg$ , so that  $f' = h'g + hg'$ . Either  $h \mid g$  or  $h' = 0$ . In the former case, we have that  $h \mid g \implies h^2 \mid f \implies f$  has a double root in  $L = K[x]/(h)$ . In the latter case, we see that  $\text{char } K = p > 0$  and  $h(x) = a_0 + a_1x^p + a_2x^{2p} + \dots + a_sx^{sp}$  with  $a_s \neq 0$ . Let  $L \supset K$  be a finite field extension such that for any  $i = 0, \dots, s$ , we have  $b_i$  such that  $b_i^p = a_i$ . Then viewing  $h(x) \in L[x]$ , we get  $h(x) = (b_0 + b_1x + b_2x^2 + \dots + b_sx^s)^p$  since  $b_s \neq 0$ . Hence if  $\varphi(x)$  is an irreducible factor of  $b_0 + b_1x + \dots + b_sx^s$  in  $L[x]$ , then if  $F = L[x]/(\varphi)$ , then  $\varphi$  has a root in  $F$  and  $h$  will have a root with multiplicity  $p$  in  $F$ . In this case,  $f$  has a root with multiplicity  $p$  in  $F$ . □

**Corollary 8.1.2.** If  $K$  has  $\text{char } K = 0$ , then every irreducible  $f(x) \in K[x]$  is separable.

*Proof.* If  $\text{char } K = 0$ , then  $f \neq 0$  and  $f$  is irreducible. Since  $\deg f > 0$ , it follows that  $f' \neq 0$ . Hence  $(f, f')$  is a polynomial of degree  $\geq 0$ . Since  $f$  is irreducible, this means that  $(f, f') \in \{1, f\}$ . But  $\deg f' < \deg f$ , so that  $(f, f') = 1$ . □

**Corollary 8.1.3.** *If  $f(x) \in K[x]$  is irreducible and  $\text{char } K \nmid \deg f$ , then  $f$  is separable.*

**Corollary 8.1.4.** *Every irreducible polynomial  $f$  over a finite field  $F$  is separable.*

*Proof.* If  $f$  is irreducible and  $f' \neq 0$ , then apply a similar argument to the proof of Corollary 8.0.4. Suppose  $f' = 0$ . Then  $f(x) = a_0 + a_1x^p + \cdots + a_sx^{sp}$  with  $p = \text{char } F$ . But as  $F$  is finite, we know that the Frobenius map  $\varphi$  is an automorphism. Thus, any element in  $F$  has a  $p$ -th root in  $F$ . Hence there exists  $b_i \in F$  such that  $b_i^p = a_i$ . This shows that  $f(x) = (b_0 + b_1x + \cdots + b_sx^s)^p$ , which contradicts that  $f$  is irreducible over  $F$ .  $\square$

**Example 8.1.5.** There are irreducible polynomials over fields of characteristic  $> 0$  that are not separable. For example, let  $K = \mathbb{F}_p(t)$  and  $f(x) = x^p - t$ . This is irreducible in  $K[x]$  but not separable over  $K$ .

Indeed, if  $L \supset K$  is such that  $f$  has a root  $\alpha$  in  $L$ , then  $f$  splits in  $L[x]$ . We can write  $f(x) = (x - \alpha)^p$ . But if  $0 < k < p$ , then  $\alpha^k \notin K$ . This shows that  $f$  is irreducible in  $F[x]$  but has a root of multiplicity  $p$ .

**Theorem 8.1.6.** *If  $f(x) \in K[x]$  and every irreducible factor of  $f$  is separable over  $K$ , then the splitting field  $L$  of  $f$  is Galois over  $K$ .*

*Proof.* We constructed  $L$  as a tower

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = L$$

where  $K_{i+1} = K_i(\alpha_{i+1})$  and  $\alpha_{i+1}$  is a root of some irreducible factor  $f_{i+1}(x)$  of  $f(x) \in K_i[x]$ . Since  $f_{i+1}$  is irreducible in  $K_i[x]$  and  $f_{i+1} \mid f$  in  $K_i[x]$ , it follows that  $f_{i+1}$  must divide one of the irreducible factors of  $f(x)$  in  $K[x]$ . But these are separable, which implies that  $f_{i+1}$  is separable for each  $i$ . By Lemma 4.2.8, a field homomorphism  $\varphi : K \rightarrow L$  extends to an isomorphism  $\varphi : L \rightarrow L$  in

$$(\# \text{ of distinct roots in } f_1) \cdot (\# \text{ of distinct roots in } f_2) \cdots (\# \text{ of distinct roots in } f_{s-1})$$

many ways. Note that  $(\# \text{ of distinct roots in } f_1) \cdot (\# \text{ of distinct roots in } f_2) \cdots (\# \text{ of distinct roots in } f_{s-1}) = \deg f_1 \cdot \deg f_2 \cdots \deg f_{s-1}$ . Hence

$$|\text{Gal}(L/K)| = \deg f_1 \cdot \deg f_2 \cdots \deg f_{s-1} = [K_1 : K_0][K_2 : K_1] \cdots [K_s : K_{s-1}] = [L : K].$$

$\square$

If  $f(x) \in K[x]$  and  $L \supset K$  is the splitting field for  $f$ , then let  $\alpha_1, \dots, \alpha_m$  denote the distinct roots of  $f$  in  $L$ . We have that  $L = K(\alpha_1, \dots, \alpha_m)$  and any  $\varphi \in \text{Gal}(L/K)$  sends  $\{\alpha_1, \dots, \alpha_m\}$  to itself. This gives us a homomorphism  $\text{Gal}(L/K) \rightarrow S_m$  that is injective by Lemma 4.2.8. Therefore,  $\text{Gal}(L/K) \subset S_m$ .

**Example 8.1.7.**

1. Let  $K$  be a field and let  $f(x) \in K[x]$  be irreducible of degree 2. Let  $L$  denote the splitting field for  $f(x)$ . Then  $K[\sqrt{D}]$  where  $D = \text{Discr}(f) \in K$ . In this case,  $[L : K] = 2$ , and  $\text{Gal}(L/K) \subset S_2$  since  $D \neq 0$ . Thus,  $f$  must have distinct roots in  $L$ . Note that  $\text{Gal}(L/K) \neq \{\text{id}\}$ , since these roots are not in  $K$ . This shows that  $\text{Gal}(L/K) = \langle \sigma \rangle = S_2$  where  $\sigma : L \rightarrow L$  is given by  $a + b\sqrt{D} \mapsto a - b\sqrt{D}$ .
2. Let  $q = p^n$ . Consider the extension  $\mathbb{F}_q \supset \mathbb{F}_p$ . Then  $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \varphi \rangle \cong \mathbb{Z}/n$ .
3. Recall that the cyclotomic field  $\Gamma_n \supset \mathbb{Q}$  is the splitting field for  $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ . This polynomial has irreducible factors each of which is separable. Thus,  $\Gamma_n \supset \mathbb{Q}$  is a Galois extension such that  $\text{Gal}(\Gamma_n/\mathbb{Q}) \subset S_{\mu_n}$ . Since any  $g \in \text{Gal}(\Gamma_n/\mathbb{Q})$  respects multiplication in  $\Gamma_n$ , we see that  $g \upharpoonright_{\mu_n} : \mu_n \rightarrow \mu_n$  is a group automorphism. It follows that  $\text{Gal}(\Gamma_n/\mathbb{Q}) \subset \text{Aut}_{\mathbf{Grp}}(\mu_n) \cong (\mathbb{Z}/n)^\times$ , which has order  $\phi(n)$ . We have shown that the minimal polynomial of a root of 1 over  $\mathbb{Q}$  is precisely  $\Phi_n(x)$ , where  $\deg \Phi_n(x) = \phi(n)$ . Hence  $[\Gamma_n : \mathbb{Q}] = \phi(n)$ , so that  $\text{Gal}(\Gamma_n/\mathbb{Q}) = (\mathbb{Z}/n)^\times$ .
4. Suppose that  $\text{char } K \notin \{2, 3\}$ . Let  $f(x) \in K[x]$  be irreducible and monic of degree 3. Let  $D \in K$  denote the discriminant of  $f$ . Let  $L \supset K$  be the splitting field for  $f$ , so that  $L \supset K$  is Galois. Then

$$|\text{Gal}(L/K)| = \begin{cases} 6 & D \notin K^2 \\ 3 & D \in K^2 \end{cases}.$$

But  $\text{Gal}(L/K) \subset S_3$ . This shows that

$$\text{Gal}(L/K) = \begin{cases} S_3 & D \notin K^2 \\ A_3 & D \in K^2 \end{cases}.$$

## 8.2 Lecture 17

**Definition 8.2.1.** Let  $k$  be a field and  $A$  be a finitely generated  $k$ -algebra. A collection  $u_1, \dots, u_n \in A$  is a *transcendence basis* of  $A/k$  if

- (i) the  $u_i$  are independent transcendentals over  $k$  and
- (ii) every  $a \in A$  is algebraically dependent with  $k[u_1, \dots, u_n]$ .

If  $A$  is a domain and  $u_1, \dots, u_n$  forms a transcendence basis of  $A/k$ , then they also form a transcendence basis of  $\text{Frac}(A)$  over  $k$ . Observe that  $x \in \text{Frac}(A)$  is algebraic over  $k[u_1, \dots, u_n]$  if and only if it is algebraic over  $k(u_1, \dots, u_n)$ . Then

$$S := \{x \in \text{Frac}(A) \mid x \text{ is algebraic over } k[u_1, \dots, u_n]\}$$

is a subfield. But  $A \subset S \subset \text{Frac}(A)$ , so that, by the universal property,  $S = \text{Frac}(A)$ . Hence  $\text{Frac}(A)$  is algebraic over  $k(u_1, \dots, u_n)$ .

Let  $A = k[u_1, \dots, u_n]$  and suppose that  $\{u_1, \dots, u_d\}$  is a maximal subset of algebraically independent elements over  $k$  in  $\{u_1, \dots, u_n\}$ . Then  $u_1, \dots, u_d$  form a transcendence basis of  $A/k$ . Indeed,  $K$

equals the algebraic closure of  $k(u_1, \dots, u_d)$  in  $\text{Frac}(A)$ . Thus,  $u_1, \dots, u_n \in K$ , so that  $K = \text{Frac}(A)$ . It follows that  $K \supset A$ .

As a result, if  $A$  is a finitely generated algebra without zero divisions, then  $A$  has a transcendence basis over  $k$ . Indeed, choose any system of generators of  $A/k$  and then choose a maximal subset of algebraically independent elements.

**Lemma 8.2.2.** *Suppose that  $\{u_1, \dots, u_n\}$  is a transcendence basis of  $A/k$  and that  $v$  is transcendental over  $k[u_1, \dots, u_n]$ . Then  $\{v, u_2, u_3, \dots, u_n\}$  is also a transcendence basis of  $A/k$ .*

*Proof.* Note that  $v, u_2, \dots, u_n$  are algebraically independent over  $k$  whereas  $v, u_1, u_2, \dots, u_n$  are algebraically dependent. A nontrivial algebraic relation among these will be given by a polynomial  $p(x)$  over  $k$  such that  $p(x)$  includes a monomial involving  $u_1$  with a nonzero coefficient. Then  $p(x)$  can be viewed as a nonzero polynomial in  $(k[v, u_1, \dots, u_n])[u_1]$  with  $\deg \geq 1$  on  $u_1$ . We have that  $u_1$  is algebraic over  $k[v, u_1, \dots, u_n]$ . Thus, the algebraic closure of  $k[v, u_2, \dots, u_n]$  in  $\text{Frac}(A)$  contains  $u_1$ , hence contains  $A$ . It follows that the algebraic closure of  $k[v, u_2, \dots, u_n]$  equals  $\text{Frac}(A)$ .

This shows that any transcendence basis of  $A/k$  has the same cardinality. Indeed, let  $u_1, \dots, u_n$  and  $v_1, \dots, v_m$  be transcendence bases of  $A/k$ . Then at least one of the  $v_i$ 's must be transcendental over  $k[u_2, \dots, u_n]$ . This is because if each  $v_i$  is algebraic over  $k[u_2, \dots, u_n]$ , then  $A \supset k[u_2, \dots, u_n]$  will be algebraic, in which case  $u_2, \dots, u_n$  is also a basis, a contradiction.

Say that  $v_1$  is transcendental over  $k[u_2, \dots, u_n]$ . Then  $A \supset k[v_1, u_2, \dots, u_n]$  is algebraic. . . . One of  $v_1, \dots, v_m$  must be transcendental over  $k[v_1, \dots, u_2, \dots, u_n]$ . Hence  $A \supset k[v_1, v_2, u_3, \dots, u_n]$  is algebraic. If  $m \leq n$ , then  $A \supset k[v_1, v_2, \dots, v_m, u_{m+1}, \dots, u_n]$  is algebraic and  $v_1, v_2, \dots, v_m, u_{m+1}, \dots, u_n$  are dependent. This is a contradiction unless  $n = m$ .  $\square$

If  $F$  is a field and  $\tilde{F} \supset F$  is a field extension, then we can measure how far  $\tilde{F}$  is from being an algebraic extension of  $F$  by its *transcendence degree over  $F$*

$$\text{trdeg}(\tilde{F}/F) \equiv \text{card}(\text{independent transcendentals we need to add to } F \text{ to generate } \tilde{F}).$$

**Corollary 8.2.3.** *trdeg is an invariant of the extension  $\tilde{F}$ .*

**Example 8.2.4.** Let  $k$  be a field and  $a_1, a_2, \dots, a_n$  be indeterminates. Let  $K := k(a_1, \dots, a_n)$ . Consider  $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n \in K[x]$ . Then  $\text{Gal}(L/K) = S_n$  where  $L$  denotes the splitting field for  $f$ .

*Proof.* Let  $x_1, x_2, \dots, x_n \in L$  denote the roots of  $f$ . Then  $a_i = (-1)^i \sigma_i(x_1, \dots, x_n)$  where  $\sigma_i$  denotes the  $i$ -th elementary symmetric function. Hence  $L = K(x_1, \dots, x_n) = k(x_1, \dots, x_n)$ . Consider the chain of field extensions  $L \supset K \supset k$ . Note that  $L \supset K$  is an algebraic extension and that  $K \supset k$  is a transcendental extension because  $K$  is obtained from adding  $n$  independent transcendentals to  $k$ .

Since  $\text{trdeg}(L/k) = \text{trdeg}(K/k) = n$  and  $L = K(x_1, \dots, x_n)$ , we see that  $x_1, \dots, x_n$  are algebraically independent over  $k$ . Therefore, there are pairwise distinct. This shows that  $f(x) \in K[x]$  has



distinct roots, so that  $L \supset K$  is separable and thus a Galois extension. It follows that  $\text{Gal}(L/K) = S_n$  and

$$L^{S_n} = (k(x_1, \dots, x_n))^{S_n} = K = k(\sigma_1, \dots, \sigma_n).$$

□

**Theorem 8.2.5 (Main theorem of Galois theory).** *Let  $L \supset K$  be a Galois extension. Then the mappings*

$$(K \subset P \subset L : P \text{ field}) \mapsto (G \leq \text{Gal}(L/K))$$

$$L^G \leftrightarrow G$$

*are inverse to each other.*

*Furthermore, if  $L \supset P \supset K$ , then  $P \supset K$  is a Galois extension of  $K$  if and only if  $\text{Gal}(L/P) \trianglelefteq \text{Gal}(L/K)$ .*

*Proof.* Consider  $K \subset P \subset L$  and  $K \subset L^{\text{Gal}(L/P)} \subset L$ . Then  $L^{\text{Gal}(L/P)} \supset P$ . From a theorem from two lectures ago, we have the following two results.

- (a)  $[L : P] = |\text{Gal}(L/P)|$  for any  $K \subset P \subset L$ .
- (b)  $[L : L^G] = |G|$  for any  $G \leq \text{Gal}(L/K)$ .

Therefore,  $[K : L^{\text{Gal}(L/P)}] \cdot [L : P] = [L : P]$ , so that  $[L^{\text{Gal}(L/P)} : L] = 1$ . Hence  $L^{\text{Gal}(L/P)} = L$ . Similarly,  $\text{Gal}(L/L^G) \leq G$  satisfies  $|\text{Gal}(L/L^G)| = |G|$ , so that  $\text{Gal}(L/L^G) = G$ .

For the second part our theorem, note that any automorphism of  $P/K$  will extend to an automorphism of  $L/K$ . This shows that the map  $\{\varphi \in \text{Gal}(L/K) \mid \varphi(P) \subset P\} \rightarrow \text{Gal}(P/K)$  given by  $\varphi \mapsto \varphi|_P$  is surjective. Then  $P \supset K$  will be Galois if and only if the elements of  $\{\varphi \in \text{Gal}(L/K) \mid \varphi(P) \subset P\}$  induce  $[P : K]$  distinct elements of  $\text{Gal}(P/K)$ .

We compute

$$|\text{Gal}(L/P)| = [L : P]$$

$$[P : K] = \frac{[L : K]}{[L : P]} = \frac{|\text{Gal}(L/K)|}{|\text{Gal}(L/P)|}$$

$$[P : K] = [\text{Gal}(L/K) : \text{Gal}(L/P)].$$

Thus,  $P \supset K$  is a Galois extension if and only if any element of  $\text{Gal}(L/K)$  leaves  $P$  invariant. But  $P = L^{\text{Gal}(L/P)}$ , and  $P = P^{\text{Gal}(L/P)}$ . Hence any  $g \in \text{Gal}(L/P)$  satisfies

$$g(P) = g(L^{\text{Gal}(L/P)}) = L^{g \text{Gal}(L/P) g^{-1}}.$$

It follows that  $g(P) = P \iff g \text{Gal}(L/P) g^{-1} = \text{Gal}(L/P)$ .

□

### 8.3 Lecture 18

**Example 8.3.1.** Let  $K$  be a field with  $\text{char } K \notin \{2, 3\}$ . Let  $f$  be an irreducible, monic, cubic polynomial over  $K$ . Let  $L$  be the splitting field for  $f$ . Let  $D := \text{Discr } f \in K \setminus K^2$ . Then  $\text{Gal}(L/K) = S_3$ . We get

$$\begin{aligned} L &\supset L^{A_3} \supset K \\ \text{Gal}(L/K) &\supseteq A_3 \supseteq \{e\}. \end{aligned}$$

It follows that  $L^{A_3} \supset K$  is Galois with  $\text{Gal}(L^{A_3}/K) \cong \text{Gal}(L/K)/A_3 \cong C_2$ . In fact,  $L^{A_3} \cong K[\sqrt{D}]$ .

Now, let  $p > 2$  be prime. Consider the cyclotomic field  $\Gamma_p \supset \mathbb{Q}$ . We have that

$$\text{Gal}(\Gamma_p/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1).$$

Let  $H \trianglelefteq \text{Gal}(\Gamma_p/\mathbb{Q})$  be the unique subgroup of index 2. Then  $[\Gamma_p^H : \mathbb{Q}] = 2$ .

Let  $\langle \varphi \rangle = \text{Gal}(\Gamma_p/\mathbb{Q})$ . Then  $\varphi \upharpoonright_{\mu_p} : \mu_p \rightarrow \mu_p$  is a group automorphism and uniquely determines  $\varphi$ , which in turn is uniquely determined by the image of  $\zeta$  the positive  $p$ -th root of 1. Write  $\varphi(\zeta) = 1\zeta^r$  for some  $r \in \mathbb{Z}_{>0}$  so that  $[r]_p \in \mathbb{Z}/p$  is a generator of  $(\mathbb{Z}/p)^\times$ .

**Definition 8.3.2.** Given  $k \in \mathbb{Z}_{>0}$  and prime  $p > 2$ , define the *Legendre symbol*

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & [k]_p \in ((\mathbb{Z}/p)^\times)^2 \\ -1 & [k]_p \notin ((\mathbb{Z}/p)^\times)^2 \end{cases}.$$

Consider  $\alpha \in \Gamma_p$  given by

$$\alpha = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{r^{k-1}} = \zeta - \zeta^r + \zeta^{r^2} - \cdots \zeta^{r^{p-2}}.$$

If  $g \in \text{Gal}(\Gamma_p/\mathbb{Q})$ , then

$$g(\alpha) = \begin{cases} \alpha & g \in H \\ -\alpha & g \notin H \end{cases}.$$

Then  $\alpha \in \Gamma_p^H$ . Also,  $\alpha^2$  is fixed by every element of  $\text{Gal}(\Gamma_p/\mathbb{Q})$  and thus is rational. This implies that  $\Gamma_p^H = \mathbb{Q}[\alpha]$ .

**Lemma 8.3.3.**  $\alpha^2 = (-1)^{\frac{p-1}{2}} p$ , so that

$$\Gamma_p^H = \begin{cases} \mathbb{Q}[\sqrt{p}] & p \equiv 1 \pmod{4} \\ \mathbb{Q}[\sqrt{-p}] & p \not\equiv 1 \pmod{4} \end{cases}.$$

*Proof.* Let  $L \supset K$  be a finite extension of fields. Then for any  $u \in L$ , we get a map  $\text{mult}_u : L \rightarrow L$ , which is linear over  $K$ . Applying trace determines a  $K$ -linear map  $L \rightarrow K$  given by  $u \mapsto \text{tr}(\text{mult}_u)$ . This induces a symmetric bilinear map  $\langle \cdot, \cdot \rangle : L \otimes_K L \rightarrow K$  given by  $u \otimes v \mapsto \text{tr}(\text{mult}_u \circ \text{mult}_v)$ . Note that if  $u \neq 0$ , then

$$\langle u, u^{-1} \rangle = \text{tr}(\text{mult}_{uu^{-1}}) = \text{tr}(\text{id}_L) = [L : K]$$

since  $(\text{char } K, [L : K]) = 1$ . Now, the vector space  $\Gamma_p$  has a  $\mathbb{Q}$ -basis  $\{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$ . Hence  $\text{mult}_{\zeta^2}$  is a cyclic operator, and  $\text{tr}(\text{mult}_1) = p - 1$  and  $\text{tr}(\text{mult}_{\zeta^k}) = -1$  for each  $k = 1, \dots, p - 2$ . It follows that

$$\langle \zeta^k, \zeta^l \rangle = \begin{cases} p - 1 & k + l \equiv 0 \pmod{p} \\ 1 & \text{otherwise} \end{cases}.$$

If  $x = \sum_{i=0}^{p-1} x_i \zeta^i$  and  $y = \sum_{i=0}^{p-1} y_i \zeta^i$  are two elements of  $\Gamma_p$ , then we can choose  $x_i$  and  $y_i$  such that  $\sum x_i = 0$  and  $\sum y_i = 0$ . Thus,

$$\langle x, y \rangle = p(x_0 y_0 + \sum k = 1^{p-1} x_k y_{p-k}).$$

But  $\alpha = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{r^{k-1}}$ , so that

$$\begin{aligned} \alpha^2 &= \frac{1}{p-1} \langle \alpha, \alpha \rangle = \frac{1}{p-1} \sum_{k=1}^{p-1} p \left(\frac{k}{p}\right) \left(\frac{-k}{p}\right) \\ &= \frac{p}{p-1} \sum_{k=1}^p \left(\frac{k}{p}\right) \left(\frac{-k}{p}\right) \\ &= p \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} p. \end{aligned}$$

□

**Definition 8.3.4.** Let  $L \supset K$  be a field extension and  $\alpha \in L$ . We say that  $\alpha$  can be expressed in radicals over  $K$  if it can be obtained from elements in  $K$  by applying  $+$ ,  $\cdot$ , and  $\sqrt[n]{\phantom{x}}$ , i.e., there exists a tower of subfields

$$K = K_0 \subset K_1 \subset \dots \subset K_s \subset L$$

such that  $K_{i+1} = K_i(\alpha_{i+1})$  where  $\alpha_{i+1}^{r_{i+1}} \in K_i$  and  $\alpha \in K_s$ .

**Proposition 8.3.5.** If  $f(x) \in K[x]$  is irreducible,  $L \supset K$  is an extension, and  $\alpha$  is a root of  $f(x)$ , then  $\alpha$  can be expressed in radicals if and only if any root of  $f$  can be expressed in radicals in the splitting field for  $f$ .

*Proof.* If  $L_1, L_2 \supset K$  are field extensions and  $\alpha_1 \in L_1$  and  $\alpha_2 \in L_2$  are roots of  $f$ , then by Lemma 4.2.8 there is a unique map  $\varphi : K(\alpha_1) \xrightarrow{\cong} K(\alpha_2)$  such that  $\varphi(\alpha_1) = \alpha_2$ . Now transport all suitable expressions by  $\varphi$  or  $\varphi^{-1}$ . □

## 9 Solvability in radicals

**Definition 9.0.1.** We say that  $f(x) \in K[x]$  is solvable in radicals if every root of  $f$  can be expressed in radicals over  $K$ .

This is equivalent to saying that  $L$  is a splitting field for  $f$ , then there is a tower of subfields  $K = K_0 \subset K_1 \subset \dots \subset K_s = L$  such that  $K_{i+1} = K_i(\alpha_{i+1})$  where  $\alpha_{i+1}^{r_{i+1}} \in K_i$ .

**Theorem 9.0.2.** *If  $K$  is a field with characteristic 0,  $f(x) \in K[x]$  is irreducible, and  $L \supset K$  is the splitting field for  $f$ , then  $f$  is solvable in radicals over  $K$  if and only if  $\text{Gal}(L/K)$  is solvable.*

**Note 9.0.3.**

1. A generic polynomial equation over  $K$  of  $\deg \geq 5$  will not be solvable in radicals, since  $\text{Gal} \cong S_n$ .
2. If  $f(x) \in \mathbb{Q}[x]$  is irreducible of degree 5, then  $f$  will not be solvable in radicals as soon as  $\text{Gal}(L/\mathbb{Q}) \in \{S_5, A_5\}$ . Suppose  $f \in \mathbb{Q}[x]$  is such a polynomial and let  $\alpha_1, \dots, \alpha_5$  be the roots of  $f$ . Note that  $\text{Gal}(L/\mathbb{Q}) \subset S_5$ . Since  $f$  is irreducible, it must be separable, which means that the  $\alpha_i$  are pairwise distinct. Hence  $5 \mid |\text{Gal}(L/\mathbb{Q})|$ . Therefore,  $\text{Gal}(L/\mathbb{Q})$  must contain an element of order 5, so that  $\text{Gal}(L/\mathbb{Q})$  contains a 5-cycle. If we can choose  $f$  so that  $\text{Gal}(L/\mathbb{Q})$  contains a transposition, then  $\text{Gal}(L/\mathbb{Q}) = S_5$ .

Choose  $f$  so that it has exactly three real roots. In this case, complex conjugation will belong to  $\text{Gal}(L/\mathbb{Q})$ , so that  $\text{Gal}(L/\mathbb{Q}) = S_5$ . Start with  $x^5 - 16x = x(x-2)(x+2)(x^2+4)$ , which has exact three real roots. To make this irreducible, shift its graph to obtain the polynomial  $f(x) = x^5 - 16x + 2$ .

## 9.1 Lecture 19

**Theorem 9.1.1.** *If  $K$  is a field with characteristic 0,  $f(x) \in K[x]$  is irreducible, and  $L \supset K$  is the splitting field for  $f$ , then  $f$  is solvable in radicals over  $K$  if and only if  $\text{Gal}(L/K)$  is solvable.*

*Proof.*

( $\Leftarrow$ )

We have a series

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \dots \supseteq G^{(s)} \supseteq \{e\},$$

which we can refine to get a normal series

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_r = \{e\}$$

such that  $G_{i+1}/G_i \cong \mathbb{Z}/n_i$ . Letting  $K_i = L^{n_i}$ , we have a tower

$$K = K_0 \subset K_1 \subset \dots \subset K_r = L.$$

Let  $F$  be the cyclotomic field that contains all roots of 1 of order  $n = n_1 n_2 \dots n_r$ . Consider the tower

$$KF \subset K_1 F \subset \dots \subset K_r F = LF.$$

Then  $K_{n_i} F \supset K_1 F$  is a cyclic extension of degree dividing  $n_i$ .

**Lemma 9.1.2.** *Let  $K$  be a field and let  $n$  have  $\text{char } K \nmid n$ . Suppose that  $K \supset \mu_n$ .*

- (a) *For any  $\alpha \in K$ , the extension  $K(\sqrt[n]{\alpha}) \supset K$  is cyclic of order dividing  $n$ .*
- (b) *For every  $\tilde{K} \supset K$  Galois and cyclic of order  $n$ , there exists  $\alpha \in K$  such that  $\tilde{K} \cong K(\sqrt[n]{\alpha})$ .*

Before proving this, note that (b) implies that  $K_{i+1}F \supset K_iF$  for every  $i$ .

*Proof.*

- (a) By definition,  $K(\sqrt[n]{\alpha})$  contains some root of  $x^n - \alpha$ . But  $K$  contains  $\mu_n$ , so that  $K(\sqrt[n]{\alpha})$  contains every root of  $x^n - \alpha$ . Thus,  $K(\sqrt[n]{\alpha})$  is the splitting field for  $x^n - \alpha$ . Hence  $K(\sqrt[n]{\alpha}) \supset K$  is Galois. If  $\sigma \in \text{Gal}(K(\sqrt[n]{\alpha})/K)$ , then  $\sigma(\sqrt[n]{\alpha}) = \zeta_\sigma \sqrt[n]{\alpha}$  where  $\zeta_\sigma$  is some  $n$ -th root of 1 depending on  $\sigma$ . Then we get a map

$$\zeta : \text{Gal}(K(\sqrt[n]{\alpha})/K) \rightarrow \mu_n$$

given by  $\sigma \mapsto \zeta_\sigma$ . But since  $K \supset \mu_n$ , if  $\sigma, \tau \in \text{Gal}(K(\sqrt[n]{\alpha})/K)$ , then

$$\sigma(\tau(\sqrt[n]{\alpha})) = \sigma(\zeta_\tau \sqrt[n]{\alpha}) = \sigma(\zeta_\tau) \sigma(\sqrt[n]{\alpha}).$$

As  $\zeta_\tau \in \mu_n \subset K$ , we see that  $\sigma(\zeta_\tau) = \zeta_\tau$ . This implies that

$$\sigma(\tau(\sqrt[n]{\alpha})) = \zeta_\tau \zeta_\sigma \sqrt[n]{\alpha}.$$

But  $\sigma(\tau(\sqrt[n]{\alpha})) = \zeta_{\tau\sigma} \sqrt[n]{\alpha}$  as well, so that  $\zeta_{\tau\sigma} = \zeta_\tau \zeta_\sigma$ . This shows that  $\zeta$  is a homomorphism.

Moreover, if  $\sigma \in \ker \zeta$ , i.e.,  $\zeta_\sigma = 1$ , then  $\sigma(\sqrt[n]{\alpha}) = 1 \cdot \sqrt[n]{\alpha} = \sqrt[n]{\alpha}$ . Since any  $\sigma \in \text{Gal}(K(\sqrt[n]{\alpha})/K)$  preserving  $\sqrt[n]{\alpha}$  must be the identity, it follows that  $\zeta$  is injective. As a result, we get an embedding  $\text{Gal}(K(\sqrt[n]{\alpha})/K) \leq \mu_n$ .

- (b) Suppose that  $\text{Gal}(\tilde{K}/K)$  is cyclic of order  $d \mid n$ . We want to show that there exists  $\alpha \in K$  such that  $\tilde{K} \cong K(\sqrt[d]{\alpha})$ .

Let  $\alpha \in \tilde{K}$  and  $\xi \in \mu_d \subset \mu_n \subset K$ . The *Lagrange resolvent* of  $(\alpha, \xi)$  is the element

$$\ell(\alpha, \xi) = \alpha + \xi \sigma(\alpha) + \xi^2 \sigma^2(\alpha) + \cdots + \xi^{d-1} \sigma^{d-1}(\alpha)$$

of  $\tilde{K}$  where  $\sigma \in \text{Gal}(\tilde{K}/K)$  is a generator.

Note that  $\sigma(\ell(\alpha, \xi)) = \xi^{-1} \ell(\alpha, \xi)$ , so that  $\sigma(\ell(\alpha, \xi)^2) = \xi^{-k} \ell(\alpha, \xi)^k$ .

Suppose that  $\xi$  is a primitive  $d$ -th root of unity. We see that  $\text{id} + \xi \sigma + \xi^2 \sigma^2 + \cdots + \xi^{d-1} \sigma^{d-1}$  is a linear combination of operators  $L \rightarrow L$  viewed as a  $K$ -vector space. But in  $\text{End}_K(\tilde{K})$  the generators are linearly independent. Therefore, module this statement, we have that

$$\sum_{k=0}^{d-1} \xi^k \sigma^k \neq 0$$

in  $\text{End}_K(\tilde{K})$ . Hence there exists  $\alpha \in \tilde{K}$  such that  $\ell(\alpha, \xi) = \sum_{k=0}^{d-1} \xi^k \sigma^k(\alpha) \neq 0$ . But for each  $i = 0, \dots, d-1$ , we see that  $\sigma^i(\ell(\alpha, \xi)) = \xi^{-i} \ell(\alpha, \xi)$ . This implies that

$$\ell(\alpha, \xi), \sigma(\ell(\alpha, \xi)), \sigma^2(\ell(\alpha, \xi)), \dots, \sigma^{d-1}(\ell(\alpha, \xi))$$

are pairwise distinct in  $\tilde{K}$ . Therefore,  $\ell(\alpha, \xi) \in \tilde{K}$  does not belong to any proper subfield of  $\tilde{K}$ .

It follows that  $\tilde{K} = K(\ell(\alpha, \xi))$ . But  $\sigma(\ell(\alpha, \xi)^d) = \underbrace{\xi^{-1}}_1 \ell(\alpha, \xi)^d = \ell(\alpha, \xi)^d$ . Hence

$$\ell(\alpha, \xi)^d = \tilde{K}^{\text{Gal}(\tilde{K}/K)} = K.$$

This proves our lemma modulo the statement that  $\text{id}, \sigma, \sigma^2, \dots, \sigma^{d-1}$  are linearly independent linear operators.

**Note 9.1.3.** The  $\sigma^i$  belong to  $\text{End}_K(\tilde{K})$  and commute with each other. They can be simultaneously diagonalized over  $L \supset K$  the splitting field for  $f(x) = \det(\sigma - x \cdot \text{id})$ . Writing a linear combination of the  $\sigma^i$  and evaluating it on a basis of eigenvectors will produce a homogenous linear system with a Vandermonde coefficient matrix. Then one needs to show that  $\sigma$  has distinct eigenvalues.

□

( $\implies$ )

See Section 9.2.

□

## 9.2 Lecture 20

**Definition 9.2.1.** If  $G$  is a group and  $k$  a field, then a  $k$ -character of  $G$  is a group homomorphism  $\chi : G \rightarrow \text{GL}_1(k) = k^\times$ .

Each  $k$ -character  $\chi$  of  $G$  can be viewed as a function with values in  $k$ .

**Lemma 9.2.2 (Dedekind).** If  $\chi_1, \dots, \chi_s$  are pairwise distinct  $k$ -characters of  $G$ , then they are linearly independent in  $\text{Fun}(G, k)$ .

*Proof.* We induct on  $s$ . If  $s = 1$ , then  $\chi_1$  must be linearly independent since  $\chi_1 \neq 0$ . Suppose, inductively, that any collection  $\sigma_1, \dots, \sigma_t$  of characters with  $t \leq s$  is linearly independent. Suppose that  $\chi_1, \dots, \chi_s$  are linearly dependent. Then there are  $a_1, \dots, a_s \in k$  such that  $a_1\chi_1 + \dots + a_s\chi_s$  is the zero function. By our IH, each  $a_i$  must be nonzero, say,  $a_s$ . Let  $b_i = -\frac{a_i}{a_s}$ . Then

$$\sum_{i=1}^{s-1} b_i \chi_i = \chi_s.$$

If  $g, h \in G$ , then

$$\chi_s(h)\chi_s(g) = \sum_{i=1}^{s-1} b_i \chi_i(h)\chi_i(g),$$

in which case  $\chi_s(g) = \sum_{i=1}^{s-1} (b_i \frac{\chi_i(h)}{\chi_s(h)}) \chi_i(g)$ . Fix  $h \in G$ , so that

$$\chi_s = \chi_s = \sum_{i=1}^{s-1} (b_i \frac{\chi_i(h)}{\chi_s(h)}) \chi_i$$

and  $\chi_s = \sum_{i=1}^{s-1} b_i \chi_i$ . It follows that  $0 = \sum_{i=1}^{s-1} (b_i \frac{\chi_i(h)}{\chi_s(h)} - b_i) \chi_i$ . By our IH, we see that  $b_i \frac{\chi_i(h)}{\chi_s(h)} - b_i = 0$ . But  $b_i \neq 0$  for any  $i$ . We have that  $\chi_i(h) = \chi_s(h)$  for any  $i = 1, \dots, s-1$ . This proves that  $\chi_i = \chi_s$  for any  $i = 1, \dots, s-1$ . This contradicts the assumption that the  $\chi_1, \dots, \chi_s$  are pairwise distinct. □

**Definition 9.2.3.** If  $K_1, K_2 \subset L$ , then the *composite* of  $K_1$  and  $K_2$  in  $L$  is the field

$$K_1 K_2 = \bigcap \left\{ P \mid P \subset L, K_1, K_2 \subset P \right\}.$$

Let  $K_1$  and  $K_2$  be finite extensions of  $k$ , so that  $K_1 = k(a_1, \dots, a_s)$  and  $K_2 = k(b_1, \dots, b_t)$ . Then the field  $k(a_1, \dots, a_s, b_1, \dots, b_t)$  both contains  $K_1 K_2$  and is contained in some  $L$  such that  $K_1, K_2 \subset L$ . Hence

$$K_1 K_2 = k(a_1, \dots, a_s, b_1, \dots, b_t).$$

**Lemma 9.2.4.** Suppose that  $K$  and  $F$  are two finite field extensions of  $k$ . Then

- (a) If  $K \supset k$  is Galois, then so is  $KF \supset F$ .
- (b)  $\text{Gal}(KF/F) = \text{Gal}(K/K \cap F)$ .

*Proof.*

- (a) If  $K \supset k$  is Galois, then  $K$  is the splitting field of some separable polynomial  $f(x) \in k[x]$ . Thus,  $KF$  is the splitting field of  $f(x)$  viewed over  $F$ . But if  $f$  is separable over  $k$ , then it is separable over  $F$ . Therefore,  $KF \supset F$  is Galois.
- (b) Consider the tower of extensions  $k \subset K \subset KF$ . The main theorem of Galois theory says that  $\text{Gal}(K/k) \trianglelefteq \text{Gal}(KF/k)$  since  $K \supset k$  is assumed to be Galois. Thus, if  $\sigma \in \text{Gal}(KF/k)$ , then  $\sigma(K) \subset K$ . Indeed,  $\sigma(K) = K$  as a subfield in  $KF$  if and only if  $\sigma(K) = (KF)^{\text{Gal}(KF/K)}$ . Let  $g \in \text{Gal}(KF/K) \subset \text{Gal}(KF/k)$ . Then  $g(x) = x$  for any  $x \in K$ .

Let  $x \in K$ . Consider  $\sigma(x) \in KF$ . We must show that  $g(\sigma(x)) = \sigma(x)$  for any  $g \in \text{Gal}(KF/K)$ , i.e.,  $(\sigma^{-1}g\sigma)(x) = x$  for any  $g$ . But since  $\sigma^{-1}g\sigma \in \sigma^{-1}\text{Gal}(KF/K)\sigma$ , we see that  $\sigma^{-1}g\sigma(x) = x$  for any  $x \in K$ . Hence we get a natural homomorphism  $\rho : \text{Gal}(KF/F) \rightarrow \text{Gal}(K/k)$  given by  $\sigma \mapsto \sigma|_K$ . Note that

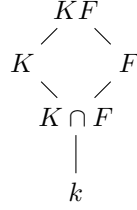
$$\begin{aligned} \ker \rho &= \{ \sigma \in \text{Gal}(KF/F) \mid \sigma|_K = \text{id}_K \} \\ &= \{ \sigma \in \text{Gal}(KF/k) \mid \sigma|_K = \text{id}_K, \sigma|_F = \text{id}_F \}. \end{aligned}$$

But  $KF$  is generated by  $K$  and  $F$ , so that  $\sigma = \text{id}_{KF}$ . This shows that  $\ker \rho = \{ \text{id}_{KF} \}$ . We see that  $\text{Gal}(KF/F) \subset \text{Gal}(K/k)$ .

Let  $H := \text{im } \rho \subset \text{Gal}(K/k)$  and consider its fixed subfield  $K^H$ . Note that (b) is equivalent to saying that  $K^H = K \cap F$ . We have that  $K^H \supset K \cap F$  because  $K^H = \{ x \in K \mid \forall \sigma \in \text{Gal}(KF/F), \sigma(x) = x \}$ . Moreover, if we view  $K^H$  as subfield of  $KF$ , then  $k \subset K^H \subset KF$  and  $k \subset F \subset KF$ . Since  $\text{Gal}(KF/F)$  fixes  $K^H$  and  $F$  (pointwise), it follows that  $\text{Gal}(KF/F)$  fixes  $K^H F$ . Therefore,  $K^H F \subset KF^{\text{Gal}(KF/F)} = F$ , so that  $K^H \subset F \cap K$ .

□

**Corollary 9.2.5.** *If both  $K$  and  $F$  are Galois field extensions of  $k$ , then*



*is a lattice of Galois field extensions.*

**Theorem 9.2.6.** *If  $K$  is a field with characteristic 0,  $f(x) \in K[x]$  is irreducible, and  $L \supset K$  is the splitting field for  $f$ , then  $f$  is solvable in radicals over  $K$  if and only if  $\text{Gal}(L/K)$  is solvable.*

*Proof.*

$(\Leftarrow)$

This was proven in Section 9.1.

$(\Rightarrow)$

For any root  $\alpha$  of  $f$ , we can find an extension  $K_\alpha \supset K$  such that  $\alpha \in L_\alpha \subset L$  and there exists a tower of radical extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = K_\alpha \subset L$$

with  $K_{i+1} = K_i(\alpha_{i+1})$  and  $\alpha_{i+1}^{n_{i+1}} \in L_i$ .

**Claim.** *Without loss of generality, we may assume that  $K_\alpha$  satisfies the following properties.*

- $\alpha \in K_\alpha$ .
- $K_\alpha \supset K$  is Galois.
- Each step of  $K_\alpha$  (viewed as our tower of radical extensions) is Galois and cyclic.

*Proof.* Since  $K_\alpha \supset K$  is a finite extension, we can find a  $K$ -basis  $e_1, \dots, e_n$  of  $K_\alpha$ . Let  $f_i \in K[x]$  denote the minimal polynomial of  $e_i$ . Let  $S_i$  denote the splitting field of  $f_i$ . Then  $S_i \supset K$  is a Galois extension and contains  $e_i$ . Note that the composite of the  $S_i$  contains each  $e_i$ . Let  $L_\alpha = S_1 S_2 \cdots S_n$ . Then  $K \subset K_\alpha \subset L_\alpha$ . (We call  $L_\alpha$  the *Galois closure* of  $K_\alpha$ .) Consider the tower  $K = K_0 \subset K_1 \subset \cdots \subset K_s = K_\alpha$  where  $K_{i+1} \supset K_i$  is a radical extension of degree  $n_i$ . If  $\sigma \in \text{Gal}(L_\alpha/K)$ , then  $K = \sigma K \subset \sigma K_1 \subset \cdots \subset \sigma K_\alpha$  is still a tower of radical extensions.

By taking the composites  $K_1 \sigma K_1 \subset \cdots \subset K_1 \sigma K_s$  and  $K_2 K_1 \sigma K_1 \cdots$ , we get a composite of all  $\{\sigma K_\alpha\}_{\sigma \in \text{Gal}(L_\alpha/K)}$ , which will be a tower of radical extensions. But  $K \subset \prod_\sigma \sigma K_\alpha \subset L_\alpha$ , and  $L_\alpha$  is generated by all  $\sigma K_\alpha$ . Hence  $L_\alpha = \prod_\sigma \sigma K_\alpha = L$ .

We still must prove that each step in our radical tower is Galois and cyclic. Let  $n = n_1 n_2 \cdots n_k$ . Let  $F = K[\mu_n]$ . If the tower  $K = K_0 \subset K_1 \subset \cdots \subset K_t = L_\alpha$  has  $K_i = K_{i-1}[\sqrt[n_i]{a_i}]$ , then we can pass to composites

$$K \subset K_0 F \subset K_1 F \subset \cdots \subset K_t F = L_\alpha F.$$



We see that  $LF \supset K$  is radical and Galois as the splitting field for  $x^n - 1$  and that  $K_i F \supset K_{i+1} F$  is radical of degree  $n_i$  and contains  $\mu_{n_i}$ . Thus,  $K_i F \supset K_{i+1} F$  is Galois and cyclic of degree dividing  $n_i$  by Lemma 8.3.3(a).

We have constructed an extension  $LF \supset K$  such that

- $\alpha \in LF$ ,
- $LF \supset L$  is Galois, and
- $LF$  is a tower of radical, cyclic, Galois extensions.

It follows that  $\text{Gal}(LF/K)$  is solvable. But  $LF \supset L \supset K$  where  $L \supset K$  is Galois. Hence  $\sigma(L) \subset L$  for any  $\sigma \in \text{Gal}(LF/K)$ , so that  $\text{Gal}(L/K) < \text{Gal}(LF/K)$ . This proves that  $\text{Gal}(L/K)$  is solvable.  $\square$

$\square$

### 9.3 Lecture 21

**Definition 9.3.1.** Let  $K$  be a field and  $f(x) \in K[x]$ . We say that  $f$  is *solvable in quadratic radicals* if the splitting field  $L$  for  $f$  is a tower

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = L$$

such that  $K_i = K_{i-1}[\sqrt{a_i}]$  for some  $a_i \in K_{i-1}$ .

**Theorem 9.3.2.** Let  $K$  be a field with  $\text{char } K \neq 2$  and  $f(x) \in K[x]$  be irreducible. Then  $f$  is solvable in quadratic radicals if and only if  $[L : K] = 2^n$  for some  $n$  where  $L$  denotes the splitting field for  $f$ .

*Proof.*

( $\implies$ )

We have that  $L \supset K$  is a tower of quadratic extensions. Hence  $[L : K] = 2^n$  for some  $n$ .

( $\impliedby$ )

We have that  $[L : K] = 2^n$  for some  $n \geq 0$  and  $\deg f = [K(\alpha) : K] \mid [L : K]$  where  $\alpha$  is a root of  $f(x)$ . Thus,  $[K(\alpha) : K]$  equals a power of 2, so that  $f$  is separable. This shows that  $L \supset K$  is Galois and thus that  $G := \text{Gal}(L/K)$  has order  $2^n$ . It follows that there is some normal series

$$G = G^0 \supseteq G^1 \supseteq \cdots \supseteq G^s = \{e\}$$

such that  $G^i / G^{i+1} \cong \mathbb{Z}/2$ . This induces a tower of field extensions

$$K = L^{G^0} \subset L^{G^1} \subset \cdots \subset L^{G^s} = L$$

such that  $[L^{G^{i+1}} : L^{G^i}] = 2$ .  $\square$

$\square$

**Note 9.3.3 (The construction problem).** Given a unit measure and segments of lengths  $a_1, \dots, a_k$ , we want to construct a segment of length  $\alpha$  using ruler and compass. Elementary geometry shows that such a construction is possible if and only if  $\alpha$  can be expressed in quadratic radicals over  $\mathbb{Q}(a_1, \dots, a_k)$ . If  $\alpha$  is transcendental over  $\mathbb{Q}(a_1, \dots, a_k)$ , then our construction is impossible.

**Example 9.3.4.** We see that  $\pi$  cannot be constructed over  $\mathbb{Q}$ , i.e., we cannot square the circle.

Moreover, if  $\alpha$  is algebraic over  $\mathbb{Q}(a_1, \dots, a_k)$ , then  $\alpha$  can be constructed by Theorem 9.3.2 if and only if the minimal polynomial of  $\alpha$  has degree power of 2.

**Example 9.3.5.**

- (a) Doubling the cube. Given a segment of length one, construct a segment of length  $\sqrt[3]{2}$ . Since the minimal polynomial of  $\sqrt[3]{2}$  is  $x^3 - 2$ , such a construction is impossible.
- (b) Trisecting an angle  $\varphi$ . Given a segment of length  $\cos \varphi$ , construct a segment of length  $\cos(\frac{\varphi}{3})$ . The minimal polynomial of  $\cos(\frac{\varphi}{3})$  over  $\mathbb{Q}(\cos \varphi)$  is  $4x^3 - 3x - \cos \varphi$ . In general, this is irreducible, in which case our construction is impossible.
- (c) Constructing regular  $n$ -gons. Given a segment of length  $i$ , construct a segment of length  $\cos(\frac{2\pi}{n})$ . This is possible if and only if  $e^{\frac{2\pi i}{n}}$  is expressible in quadratic radicals over  $\mathbb{Q}$ . In turn, this happens if and only if

$$\underbrace{[\Gamma_n : \mathbb{Q}]}_{\varphi(n)} = 2^s.$$

For example, if  $p$  is prime, then we can construct a regular  $p$ -gon if and only if  $1 + 2^k$  for some  $k$ . Currently, the largest known such  $p$  is 65,537.

## 10 Further applications of Galois theory

### 10.1 Lecture 22

To begin, note that the following statements are true.

- If  $f(x) \in \mathbb{R}[x]$  has odd degree, then it has a real root.
- Every  $\alpha \in \mathbb{C}$  has a square root in  $\mathbb{C}$ .

Now, suppose that  $K \supsetneq \mathbb{R}$  is a finite field extension. If  $[K : \mathbb{R}]$  is odd and  $\alpha \in K \setminus \mathbb{R}$ , then  $K \supset \mathbb{R}(\alpha) \supset \mathbb{R}$ , in which case  $\deg f \mid [K : \mathbb{R}]$  where  $f$  denotes the minimal polynomial of  $\alpha$  over  $\mathbb{R}$ . In this case,  $f$  has odd degree and thus has a root in  $\mathbb{R}$ , so that  $\mathbb{R}(\alpha) = \mathbb{R}$ , a contradiction. This proves that  $[K : \mathbb{R}]$  is even.

We want to prove the *fundamental theorem of algebra*: that any  $f(x) \in \mathbb{C}[x]$  has a root in  $\mathbb{C}$ . Note that if  $c$  is a complex root of  $f(x)\overline{f(x)} \in \mathbb{R}[x]$ , then either  $c$  or  $\bar{c}$  is a root of  $f(x)$ . Thus, it suffices to show that any polynomial over  $\mathbb{R}$  has a root in  $\mathbb{C}$ .

To this end, let  $g(x) \in \mathbb{R}[x]$  be non-constant and irreducible. Let  $L$  denote the splitting field for  $g$ . Then  $[L : K] = |\text{Gal}(L/\mathbb{R})|$  is even, so that there is some nontrivial 2-Sylow subgroup  $H \leq \text{Gal}(L/\mathbb{R})$ . This means that the intermediate extension  $L \supset L^H \supset \mathbb{R}$  has odd degree. But then  $L^H = \mathbb{R}$ . This means that  $L \supset L^H$  is Galois, so that

$$[L : \mathbb{R}] = [L : L^H] = |\text{Gal}(L/L^H)| = |H| = 2^n$$

for some  $n$ . By Theorem 9.3.2, it follows that  $g(x)$  is solvable in quadratic radicals. Therefore,  $L = \mathbb{C}$  since  $[\mathbb{C} : \mathbb{R}] = 2$ .

**Theorem 10.1.1 (Primitive element theorem).** *Suppose that  $L \supset K$  is a finite field extension. This has a primitive element, i.e.,  $L = K(\theta)$  for some  $\theta \in L$ , if and only if there are at most finitely many intermediate fields  $K \subset F \subset L$ .*

*Proof.* If  $K$  is finite, then  $L$  is a finite group with cyclic multiplicative group  $\langle \theta \rangle$ . In this case, we have shown that  $L = K(\theta)$ .

( $\Leftarrow$ )

For any  $\alpha, \beta \in L$ , consider the collection of intermediate fields

$$K \subset K(\alpha + c\beta) \subset L$$

where  $c \in K$ . Thus,  $\exists c, c' \in K$  such that  $E := K(\alpha + c\beta) = K(\alpha + c'\beta)$ . Hence  $(c - c')\beta \in E$ , and  $c - c' \in K \setminus \{0\}$ . Then  $\beta \in E$ , so that  $\alpha \in E$ . This shows that  $E \supset K(\alpha, \beta)$ . It's clear that  $E \subset K(\alpha, \beta)$ . Hence  $E = K(\alpha, \beta)$ . But  $L \supset K$  is a finite extension, which implies that  $L = K(\alpha_1, \dots, \alpha_n)$  for some  $\alpha_1, \dots, \alpha_n$ . By induction on  $n$ , we can find elements  $c_2, \dots, c_n \in K$  such that

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1 + c_2\alpha_2 + c_3\alpha_3 + \dots + c_n\alpha_n).$$

( $\Rightarrow$ )

We have that  $L = K(\theta)$ . Let  $f(x) \in K[x]$  denote the minimal polynomial of  $\theta$  over  $K$ . Let  $K \subset F \subset L$  be an intermediate field extension. Let  $g_F(x) \in F[x]$  denote the minimal polynomial over  $F$ . This proves that  $g_F(x) \mid f(x)$  in  $F[x]$ . We get a map

$$(\text{intermediate field extensions } K \subset F \subset L) \rightarrow (\text{divisors of } f(x))$$

given by  $F \mapsto g_F(x)$ . Since there are at most finitely many divisors of  $f(x)$ , it suffices to check that this map is injective.

Suppose that  $K \subset F \subset L$ . Let  $F_0 \subset F$  be the subfield obtained from  $K$  by adjoining the coefficients of  $g_F(x)$ . It is enough to show that  $F_0 = F$ . Note that  $g_F(x)$  is irreducible in  $F[x]$ , so that  $g_F(x)$  is irreducible in  $F_0[x]$ . Therefore,  $g_F(x) \in F_0[x]$ , which means that  $g_F(x)$  is the minimal polynomial of  $\theta$  over  $F_0$ . Then  $[L : F_0] = \deg g_F = [L : F]$ , so that  $F_0 = F$ .  $\square$

**Corollary 10.1.2.** *If  $L \supset K$  is a (finite) separable extension, then  $L$  has a primitive element.*

*Proof.* It suffices to show that if  $\alpha, \beta \in L$  are separable over  $K$ , then  $K(\alpha, \beta) = K(\theta)$  for some  $\theta$ . If  $K$  is finite, then we're done. Suppose that  $K$  is infinite. Let  $\varphi_1, \dots, \varphi_n$  denote the distinct embeddings of  $K(\alpha, \beta)$  in  $\bar{K}$  over  $K$ . Consider

$$f(x) = \prod_{i \neq j} (\varphi_i(\alpha) + x\varphi_i(\beta) - \varphi_j(\alpha) - x\varphi_j(\beta)).$$

Since this is not the zero polynomial, there is some  $c \in K$  such that  $f(c) \neq 0$ . It follows that the  $\varphi_i(\alpha + c\beta)$  are pairwise distinct in  $\bar{K}$ . Then  $[K(\alpha + c\beta) : K] \geq n$ . But  $[K(\alpha, \beta) : K] = n$ , so that  $K(\alpha, \beta) = K(\alpha + c\beta)$ .  $\square$

Let  $K$  be a field and  $f(x) \in K[x]$  be a monic separable polynomial. Let  $L$  denote the splitting field of  $f$ , so that  $L \supset K$  is Galois. Let  $G_f := \text{Gal}(L/K) \subset S_n$  where  $n = \deg f$ . Let  $\text{char } K \neq 2$ .

**Theorem 10.1.3.**  $L^{G_f \cap A_n} = K(\Delta(f))$  where  $\Delta(f) = \prod_{i < j} (\lambda_i - \lambda_j)$  and  $\lambda_1, \dots, \lambda_n$  denote the distinct roots of  $f$ .

Before proving this, note that  $\Delta(f)$  is a square root of  $\text{Discr}(f) \in K$ .

*Proof.* Consider  $x_1, \dots, x_n$  purely transcendental elements over  $K$ . Let  $K(x_1, \dots, x_n) \supset K$  be the corresponding extension. There is a group homomorphism  $\Phi : S_n \rightarrow \text{Gal}(K(x_1, \dots, x_n)/K)$  given by  $\sigma \mapsto \Phi_\sigma$  where

$$\Phi_\sigma(f)(x_1, \dots, x_n) = f(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}).$$

This is injective, and  $K(x_1, \dots, x_n)^{S_n} = K(\sigma_1, \dots, \sigma_n)$  where  $\sigma_1, \dots, \sigma_n \in K[x_1, \dots, x_n]$  are the alternating symmetric polynomials. Further,  $\text{Gal}(K(x_1, \dots, x_n)/K(\sigma_1, \dots, \sigma_n)) = S_n$ . Let  $\Delta_n = \prod_{i < j} (x_i - x_j) \in K(x_1, \dots, x_n)$ . Then  $\Phi_\sigma(\Delta_n) = \text{sgn}(\sigma)\Delta_n$ , and  $\Delta_n \notin K(\sigma_1, \dots, \sigma_n)$ .

Define  $\text{ev} : K(x_1, \dots, x_n) \rightarrow L$  by  $x_i \mapsto \lambda_i$ . Then  $\text{ev} \circ \Phi_\sigma = \sigma^{-1} \circ \text{ev}$ . Thus,

$$\text{ev}(\Delta(f)) = \text{ev}(\Phi_\sigma(\Delta_n)) = \sigma^{-1}(\Delta(f)).$$

This shows that the subgroup in  $G_f$  fixing  $\Delta(f)$  is precisely  $G_f \cap A_n$ .  $\square$

**Corollary 10.1.4.** If  $\text{char } K \neq 2$  and  $f(x)$  is monic and separable over  $K$ , then  $G_f \subset A_n$  if and only if  $\text{Discr}(f) \in K^2$ .

## 10.2 Lecture 23

**Theorem 10.2.1.** Suppose that  $K$  is a field and  $f(x) \in K[x]$  is separable. Then  $f$  is irreducible if and only if the Galois group  $G_f$  acts transitively on the set of roots of  $f$ .

*Proof.*

( $\implies$ )

For any two roots  $\lambda_i, \lambda_j$  of  $f$ , we have that  $K(\lambda_i) \cong K(\lambda_j)$  as fields over  $K$  because both  $\text{ev}_{\lambda_i} : K[x] \rightarrow K(\lambda_i)$  and  $\text{ev}_{\lambda_j} : K[x] \rightarrow K(\lambda_j)$  induces isomorphisms with  $K[x]/(f)$ . By Lemma 4.2.8, we

can extend this isomorphisms to an automorphism  $\sigma : L \rightarrow L$  of the splitting field  $L$  for  $f$ . Thus,  $\sigma \in \text{Gal}(L/K)$  with  $\sigma(\lambda_i) = \lambda_j$ .

( $\Leftarrow$ )

Let  $\{\lambda_1, \dots, \lambda_n\}$  denote the set of roots of  $f$ . Let  $f(x) = g(x)h(x)$  where  $\deg g \geq 1$  and  $g$  is irreducible. We must show that  $h$  is constant. Let  $\lambda$  be any root of  $g$ . Then there exists  $\sigma_i \in G_f$  such that  $\sigma_i(\lambda) = \lambda_i$  for each  $i = 1, \dots, n$ . Note that

$$g(\lambda_i) = g(\sigma_i(\lambda)) = \sigma_i(g(\lambda)) = 0,$$

so that each  $\lambda_i$  is a root of  $g$ . Hence  $f \mid g$ , which implies that  $h$  is constant.  $\square$

**Theorem 10.2.2.** *Suppose that  $p$  is prime and that  $f(x) \in \mathbb{Q}[x]$  is monic and irreducible with  $\deg f = p$ . Suppose that  $f$  has exactly two non-real roots in  $\mathbb{C}$ . Then  $G_f = S_p$ .*

*Proof.* Let  $L$  be the splitting field for  $f(x)$ . Write  $f(x) = \prod_{i=1}^p (x - x_i)$  with each  $\lambda_i \in \mathbb{C}$ . Then  $\mathbb{Q}(\lambda_1, \dots, \lambda_p) \subset \mathbb{C}$ . We see that

$$\mathbb{Q} \subset \mathbb{Q}(\lambda_i) \subset \mathbb{Q}(\lambda_1, \dots, \lambda_p) \subset \mathbb{C},$$

so that  $[\mathbb{Q}(\lambda_i) : \mathbb{Q}] \mid [L : \mathbb{Q}]$ . Since  $p \mid [L : \mathbb{Q}] = |G_f| \subset S_p$ , it follows from Sylow that  $G_p$  contains an element of order  $p$ , i.e., that  $G_f$  contains a  $p$ -cycle. Also, the element in  $G_f$  that switches the roots is the complex conjugate pair of a transposition.  $\square$

**Theorem 10.2.3 (Brouwer).** *For any prime  $p \geq 5$ , there are infinitely many polynomials in  $\mathbb{Q}[x]$  of degree  $p$  with Galois group  $S_p$ .*

*Proof.* Let  $k$  be an odd integer and let  $0 \leq m, n_1 \leq n_2 < \dots < n_{k-2}$  be even integers. Consider

$$g(x) = (x^2 + m)(x - n_1)(x - n_2) \cdots (x - n_{k-2}).$$

This polynomial has  $\frac{k-3}{2}$  local maxima. Also, for each odd  $h \in \mathbb{Z}$ ,  $|g(h)| > 2$ . Hence if  $c$  denotes a local maximum of  $g$ , then  $g(c) > 2$ . This shows that if  $f(x) = g(x) - 2$ , then there are

- $\frac{k-3}{2}$  positive local maxima in  $[n_1, n_{k-2}]$  and
- $\frac{k-3}{2}$  negative local maxima in  $[n_1, n_{k-2}]$ .

It follows that  $f(x)$  has  $k-3$  real roots in  $[n_1, n_{k-2}]$  with  $f(n_{k-2}) = -2$  and  $\lim_{x \rightarrow \infty} f(x) > 0$ . Therefore, we have another real roots  $> n_{k-2}$ . Hence  $f(x)$  has at least  $k-2$  real roots. Let  $\lambda, \dots, \lambda_n \in \mathbb{C}$  denote the distinct roots of  $f$ . Then

$$\prod_{i=1}^k (x - \lambda_i) = f(x) = (x^2 + m)(x - n_1)(x - n_2) \cdots (x - n_{k-2}) - 2$$

, and  $-\sum_{i=1}^k \lambda_i = -\sum_{i=1}^{k-2} n_i$ . From this, we compute

$$\begin{aligned} \sum_{i < j} \lambda_i \lambda_j &= m + \sum_{a < b} n_a n_b \\ \sum_{i=1}^k \lambda_i^2 &= \left( \sum_{i=1}^k \lambda_i \right)^2 = \sum_{i < j} \lambda_i \lambda_j \\ &= \left( \sum_{i=1}^{k-2} n_i \right)^2 - 2m - 2 \left( \sum_{a < b} n_a n_b \right) \\ &= \sum_{i=1}^{k-2} n_i^2 - 2m. \end{aligned}$$

Choose  $m \gg \sum n_i^2$ , so that  $\sum_{i=1}^k \lambda_i^2 < 0$ . This implies that there exists a non-real root. Hence we must have exactly two real roots. Further, we can write  $f(x) = x^k + a_1 x^{k-1} + \cdots + a_{k-1} x + a_k$  with each  $a_i \in 2\mathbb{Z}$ . Since  $a_k = f(0) = g(0) - 2$ , we see that  $2 \mid a_{k-1}$  but  $4 \nmid a_{k-1}$ . By Eisenstein's criterion,  $f$  must be irreducible. We thus get infinitely many  $f$ 's such that  $G_f = S_p$ .  $\square$

## 11 Chain complexes and chain maps

The originators of homological algebra include Betti, Poincaré, and Riemann. The main goal of this subject is to extract invariants from topological spaces. Decompose  $X$  into contractible pieces (such as cells or simplices) to reduce  $X$  to combinatorial data. Specifically, reduce  $X$  to a collection of pieces of various dimensions where the boundary of a piece of dimension  $n$  is glued to a sub-collection of pieces of dimension  $n - 1$ .

Emmy Noether introduced groups of chains  $C_i(X)$ , a free abelian group generated by the collection of  $i$ -dimensional pieces, equipped with boundary relations  $\partial_i : C_i(X) \rightarrow C_{i-1}(X)$ . From this, we obtain abelian groups  $H_i(X) \equiv \ker \partial_i / \text{im } \partial_{i+1}$ , which are algebraic invariants of  $X$ .

Hilbert wanted to extract numerical invariants from a module. Specifically, if  $k$  is a field and  $K := k[x_1, \dots, x_n]$ , then he wanted to understand the complexity of a module over  $K$  (or, more generally, any graded module over  $k$ ).

A typical graded module over  $R$  will be a module of the form  $MR/I$  where  $I \trianglelefteq R$  is a homogeneous ideal. By the Hilbert basis theorem,  $I \trianglelefteq R$  is generated by finitely many homogenous polynomials  $f_1, f_2, \dots, f_{r_0}$ . Thus, we have surjective map  $\psi : R^{\oplus r_0} \rightarrow I$  given by  $(a_1, \dots, a_{r_0}) \mapsto \sum a_i f_i$ . But, these generators are not, in general, independent. Therefore, we consider the module of relations  $Z_0(I) \equiv \ker \psi$  among the  $f_i$ . Note that  $Z_0(I)$  is finitely generated. We can choose generators and get a map  $\psi' : R^{\oplus r_1} \rightarrow Z_0(I)$ . Then

$$R^{\oplus r_1} \rightarrow R^{\oplus r_0} \rightarrow I \rightarrow 0$$

is an exact sequence of graded  $R$ -modules. If  $Z_1(I) \equiv \ker \psi'$  is not zero, then choose generators again to get a map  $\psi'' : R^{\oplus r_2} \rightarrow Z_1(I)$ . Continuing in this way, we get an exact sequence

$$\cdots \rightarrow R^{\oplus r_2} \rightarrow R^{\oplus r_1} \rightarrow R^{\oplus r_0} \rightarrow I \rightarrow 0.$$

The *length* of this sequence is defined to be  $\max\{i \mid r_i \neq 0\}$ . This is an invariant of  $I$  and of  $R/I$ .

**Theorem 11.0.1 (Hilbert's syzygy theorem).** *Hilbert's syzygy theorem states that  $Z_{n-1}(I)$  is free, i.e., that there is an exact sequence of graded  $R$ -modules*

$$0 \rightarrow R^{\oplus r_n} \rightarrow R^{\oplus r_{n-1}} \rightarrow \dots \rightarrow R^{\oplus r_0} \rightarrow I \rightarrow 0.$$

## 11.1 Lecture 24

### Definition 11.1.1.

1. A *chain complex* (in  $\mathbf{Ab}$ ) is a pair  $(M_\bullet, \partial_\bullet)$  where  $M_\bullet = \{M_i\}_{i \in \mathbb{Z}}$  is a set of abelian groups and  $\partial_\bullet = \{\partial_i\}_{i \in \mathbb{Z}}$  is a set of morphisms in  $\mathbf{Ab}$  such that the  $i$ -th differential  $\partial_i : M_i \rightarrow M_{i-1}$  satisfies  $\partial_{i-1} \circ \partial_i = 0$ .

We call  $Z_n \equiv \ker \partial_n$  the *group of degree  $n$  cycles* and  $B_n \equiv \operatorname{im} \partial_{n+1}$  the *group of degree  $n$  boundaries*. Finally, we call  $H_n \equiv Z_n/B_n$  the *degree  $n$  homology group*.

2. A *((co)chain) complex* (in  $\mathbf{Ab}$ ) is a pair  $(M^\bullet, d^\bullet)$  where  $M^\bullet = \{M^i\}_{i \in \mathbb{Z}}$  is a set of abelian groups and  $d^\bullet = \{d^i\}_{i \in \mathbb{Z}}$  is a set of morphisms in  $\mathbf{Ab}$  such that the  $i$ -th differential  $d^i : M^i \rightarrow M^{i+1}$  satisfies  $d^{i+1} \circ d^i = 0$ .

We call  $Z^n \equiv \ker d^n$  the *group of degree  $n$  cocycles* and  $B^n \equiv \operatorname{im} d^{n-1}$  the *group of degree  $n$  coboundaries*.

Finally, we call  $H^n \equiv Z^n/B^n$  the *degree  $n$  cohomology group*.

**Definition 11.1.2.** Let  $(A^\bullet, d_A^\bullet)$  and  $(B^\bullet, d_B^\bullet)$  be complexes. A *chain map*  $f^\bullet : (A^\bullet, d_A^\bullet) \rightarrow (B^\bullet, d_B^\bullet)$  consists of group homomorphisms  $f^i : A^i \rightarrow B^i$  for each  $i \in \mathbb{Z}$  such that  $d_B^i \circ f^i = f^{i+1} \circ d_A^i$ .

### Note 11.1.3.

1. Any chain map  $f^\bullet : (A^\bullet, d_A^\bullet) \rightarrow (B^\bullet, d_B^\bullet)$  restricts term-wise to maps  $f^i : Z^i(A^\bullet) \rightarrow Z^i(B^\bullet)$  and maps  $f^i : B^i(A^\bullet) \rightarrow B^i(B^\bullet)$ . Thus, it induces a map  $f^* : H^i(A^\bullet) \rightarrow H^i(B^\bullet)$ .
2. We have a natural isomorphism  $\mathbf{Ch}(\mathbf{Ab}) \rightarrow \mathbf{CoCh}(\mathbf{Ab})$  given by  $N_i \mapsto M^{-i}$  and  $\partial_i \mapsto d^{-i}$ .

**Definition 11.1.4.** We say that  $(A^\bullet, d^\bullet)$  is *bounded above* if there is some  $N$  such that  $A^n = 0$  for any  $n \geq N$ . We define *bounded below* similarly. We say that  $(A^\bullet, d^\bullet)$  is *bounded* if it is both bounded above and bounded below.

As a result, we have the subcategories  $\mathbf{CoCh}^-(\mathbf{Ab})$ ,  $\mathbf{CoCh}^+(\mathbf{Ab})$ , and  $\mathbf{CoCh}^b(\mathbf{Ab})$ , respectively.

If  $C^\bullet = \bigoplus_{i \in \mathbb{Z}} C^i$  is a graded abelian group, then it induces a natural complex  $(\underline{C}^\bullet, 0)$  where  $\underline{C}^i \equiv C^i$ . In particular, any abelian group may be viewed as a complex.

Conversely, given a complex  $(M^\bullet, d^\bullet)$ , we can form the graded abelian group  $M^\bullet \equiv \bigoplus_{i \in \mathbb{Z}} M^i$  and package the differential  $d^i$  into a single group map  $D : M^\bullet \rightarrow M^\bullet$  such that  $D \upharpoonright_{M^i} = d^i$  and  $D^2 = 0$ .

We can write  $D$  as the block diagonal matrix

$$\begin{bmatrix} 0 & & & & \\ d^i & 0 & & & \\ & d^{i+1} & 0 & & \\ & & d^{i+2} & 0 & \\ & & & \ddots & \ddots \end{bmatrix}.$$

As a result, we obtain the *cochain functor* given by  $(A^\bullet, d^\bullet) \rightarrow \bigoplus_{i \in \mathbb{Z}} A^i$  and  $f^\bullet \mapsto (f^i)_{i \in \mathbb{Z}}$ .

**Definition 11.1.5.** We say that  $(A^\bullet, d^\bullet)$  is *acyclic* or *exact* if  $H^\bullet(A^\bullet, d^\bullet) = 0$ .

**Definition 11.1.6.** If  $A$  is an abelian group, then a *left resolution* of  $A$  is an exact complex  $(C^\bullet, d^\bullet) \in \text{ob } \mathbf{CoCh}^{\leq 0}(\mathbf{Ab})$  of the form

$$\cdots \rightarrow C^{i-1} \rightarrow C^i \rightarrow \cdots \rightarrow C^0 \rightarrow A \rightarrow 0.$$

**Example 11.1.7.** If  $I \trianglelefteq k[x_1, \dots, x_n]$  is a homogenous ideal, then Hilbert's syzygy theorem says that  $I$  has a left resolution of length  $n + 1$  with  $n + 1$  terms free finitely generated  $R$ -modules.

Let  $a \in \mathbb{Z}$ . Define the *shift functor*

$$-[a] : \mathbf{CoCh}(\mathbf{Ab}) \rightarrow \mathbf{CoCh}(\mathbf{Ab})$$

as follows. Let  $(M^\bullet, d_M^\bullet)$  be a complex. Form the pair  $(M^\bullet[a], d_{M[a]}^\bullet)$  where  $(M^\bullet[a])^n \equiv M^{a+n}$  and  $(d_{M[a]}^\bullet)^n \equiv (-1)^a d_M^{a+n}$ . If  $f^\bullet$  is a chain map, then let  $(f^\bullet[a])^n = f^{a+n}$ .

**Proposition 11.1.8.** *The shift functor is an equivalence that preserves  $\mathbf{CoCh}^-(\mathbf{Ab})$ ,  $\mathbf{CoCh}^+(\mathbf{Ab})$ , and  $\mathbf{CoCh}^b(\mathbf{Ab})$ .*

**Definition 11.1.9.** Let  $f : M \rightarrow N$  be a chain map. Form  $\text{cone}(f)$  the *cone of  $f$*  as a new complex where  $\text{cone}(f)^\bullet \equiv N \oplus M[1]$  and  $d_{\text{cone}(f)}^\bullet \equiv \begin{bmatrix} d_N & f \\ 0 & d_{M[1]} \end{bmatrix}$ .

We see that

$$\text{cone}(f)^n = N^n \oplus M^{n+1}$$

and  $d_{\text{cone}(f)}^n : N^n \oplus M^{n+1} \rightarrow N^{n+1} \oplus M^{n+2}$  with

$$d_{\text{cone}(f)}^n = \begin{bmatrix} d_N^n & f^{n+1} \\ 0 & -d_M^{n+1} \end{bmatrix}.$$

**Exercise 11.1.10.** *Show that  $d_{\text{cone}(f)}^{i+1} \circ d_{\text{cone}(f)}^i = 0$ .*

**Definition 11.1.11.**



1. A *double complex* is a triple  $(A^{\bullet,\bullet}, d^{\bullet}, \delta^{\bullet})$  where  $A^{i,j} = \{A^{i,j}\}_{(i,j) \in \mathbb{Z}^2}$  and both  $d : A^{\bullet,\bullet} \rightarrow A^{\bullet+1,\bullet}$  and  $\delta : A^{\bullet,\bullet} \rightarrow A^{\bullet,\bullet+1}$  are homomorphisms such that  $d\delta = \delta d$  and  $d^2 = \delta^2 = 0$ . As a commutative diagram, this has the form

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 \dots & \xrightarrow{\delta} & A^{p,q} & \xrightarrow{\delta} & A^{p,q+1} & \xrightarrow{\delta} & A^{p,q+2} \xrightarrow{\delta} \dots \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 \dots & \xrightarrow{\delta} & A^{p+1,q} & \xrightarrow{\delta} & A^{p+1,q+1} & \xrightarrow{\delta} & A^{p+1,q+2} \xrightarrow{\delta} \dots \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 \dots & \xrightarrow{\delta} & A^{p+2,q} & \xrightarrow{\delta} & A^{p+2,q+1} & \xrightarrow{\delta} & A^{p+2,q+2} \xrightarrow{\delta} \dots \\
 & & \downarrow d & & \downarrow d & & \downarrow d \\
 & & \vdots & & \vdots & & \vdots
 \end{array}$$

2. The *total complex* of  $(A^{\bullet,\bullet}, d^{\bullet}, \delta^{\bullet})$  is the complex  $\text{Tot}(A)$  where  $\text{Tot}(A)^n \equiv \bigoplus_{p+q=n} A^{p,q}$  and  $d_{\text{Tot}(A)} \upharpoonright_{A^{p,q}} \equiv d + (-1)^p \delta$ .

**Proposition 11.1.12.** *Any chain map  $f : M \rightarrow N$  induces a double complex*

$$\begin{array}{ccccccc}
 M^{i-1,0} & \xrightarrow{d_M} & M^{i,0} & \xrightarrow{d_M} & M^{i+1,0} & \xrightarrow{d_M} & M^{i+2,0} \xrightarrow{d_M} \dots \\
 \downarrow f & & \downarrow f & & \downarrow f & & \downarrow f \\
 N^{i-1,1} & \xrightarrow{d_N} & N^{i,1} & \xrightarrow{d_N} & N^{i+1,1} & \xrightarrow{d_N} & N^{i+2,1} \xrightarrow{d_N} \dots
 \end{array}$$

The total complex of this is precisely  $\text{cone}(f)$ .

Let  $N$  and  $C$  be complexes. Suppose that  $C \xrightarrow{\iota} N$  is a chain map where each  $\iota^n : N^n \rightarrow C^n$  is injective. Let  $s^n : C^n \rightarrow N^n$  be a group homomorphism such that  $s^n \circ \iota^n = \text{id}_{N^n}$ . Then  $M := (C/N, d_{C/N})$  is a complex. Our choice of  $s^n$  produces a splitting  $C^{\bullet} \cong N^{\bullet} \oplus M^{\bullet}[1]$  in the category of graded abelian groups. Thus, we have the map  $d_C = \begin{bmatrix} d_N & f \\ 0 & d_{M[1]} \end{bmatrix}$  where  $f : M \rightarrow N$  is a map of graded abelian groups.

**Exercise 11.1.13.** *Show that  $f$  is a chain map and  $C \cong \text{cone}(f)$ .*

## 11.2 Lecture 25

**Definition 11.2.1.** Let  $f, g : A^{\bullet} \rightarrow B^{\bullet}$  be two chain maps. A *homotopy between  $f$  and  $g$*  is a map of graded abelian groups  $h : A^{\bullet} \rightarrow B^{\bullet-1}$  such the

$$d_B h + h d_A = f - g.$$

We say that  $f$  and  $g$  are *homotopy equivalent* (written as  $f \sim g$ ) if there is a homotopy between them.

**Proposition 11.2.2.**

1. Homotopy is an equivalence relation.
2. The class  $\text{mor}^{\sim 0} \mathbf{CoCh}(\mathbf{Ab})$  of all chain maps homotopic to 0 is a two-sided ideal in  $\text{mor} \mathbf{CoCh}(\mathbf{Ab})$ .
3. If  $f \simeq g : A^\bullet \rightarrow B^\bullet$ , then  $H^\bullet(f) = H^\bullet(g)$ .
4. If  $f \simeq g$  and  $c$  is a cocycle, then  $f(c) - g(c) = d_B h(c)$ , which is a coboundary.

*Notation.* Let  $\mathcal{C}(\mathbf{Ab})$  denote the category with complexes as objects and homotopy classes of chain maps as morphisms.

**Note 11.2.3.**

1. We have that  $\text{Hom}_{\mathcal{C}(\mathbf{Ab})}(A, B) = \text{Hom}_{\mathbf{CoCh}(\mathbf{Ab})}(A, B) / \text{Hom}_{\mathbf{CoCh}(\mathbf{Ab})}^{\sim 0}(A, B)$ .
2.  $H^\bullet$  descends to a well-defined functor in the sense that the diagram

$$\begin{array}{ccc} \mathbf{CoCh}(\mathbf{Ab}) & \longrightarrow & \mathcal{C}(\mathbf{Ab}) \\ H^\bullet \downarrow & \swarrow H^\bullet & \\ \mathbf{grAb} & & \end{array} .$$

commutes.

**Definition 11.2.4.** A *short exact sequence of complex* is a sequence  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  of complexes such that each sequence

$$0 \rightarrow A^n \xrightarrow{f^n} B^n \xrightarrow{g^n} C^n \rightarrow 0$$

is exact in  $\mathbf{Ab}$ .

Let

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

be a short exact sequence of complexes. Consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & A^{n-1} & \xrightarrow{f^{n-1}} & B^{n-1} & \xrightarrow{g^{n-1}} & C^{n-1} \longrightarrow 0 \\ & & d_A^{n-1} \downarrow & & d_B^{n-1} \downarrow & & d_C^{n-1} \downarrow \\ 0 & \longrightarrow & A^n & \xrightarrow{f^n} & B^n & \xrightarrow{g^n} & C^n \longrightarrow 0 \\ & & d_A^n \downarrow & & d_B^n \downarrow & & d_C^n \downarrow \\ 0 & \longrightarrow & A^{n+1} & \xrightarrow{f^{n+1}} & B^{n+1} & \xrightarrow{g^{n+1}} & C^{n+1} \longrightarrow 0 \end{array} .$$

Define a collection of *edge homomorphisms*  $\{\delta^n : H^n(C) \rightarrow H^{n+1}(A)\}_{n \in \mathbb{Z}}$  as follows. Let  $c \in C^n$  with  $d_C^n(c) = 0$ . By exactness, there is some  $b \in B^n$  such that  $g^n(b) = c$ . But then

$$d_B^n(b) \in \ker g^{n+1} = \text{im } f^{n+1}.$$

Since  $f^{n+1}$  is injective, this means that there is a unique  $a \in A^{n+1}$  such that  $f^{n+1}(a) = d_B^n(b)$ . Let  $\delta^n([c]) = [a]$ .

**Exercise 11.2.5.** Check that  $\delta^n$  is a homomorphism and that it is independent both of our choice of  $c$  and of our choice of  $b$ .

**Lemma 11.2.6 (Snake).** Any short exact sequence

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

complexes induces a long exact sequence in cohomology

$$\begin{array}{ccccccc} & & \cdots & \longrightarrow & H^{n-1}(C) & & \\ & & \delta^{n-1} & \nearrow & & & \\ H^n(A) & \xrightarrow{f^*} & H^n(B) & \xrightarrow{g^*} & H^n(C) & \cdot & \\ & & \delta^n & \nwarrow & & & \\ H^{n+1}(A) & \xrightarrow{f^*} & H^{n+1}(B) & \longrightarrow & \cdots & & \end{array}$$

*Proof.*

Exactness at  $H^n(B)$ : We have that  $0_{H^n(C)} = H^n(0) = H^n(g \circ f) = H^n(g) \circ H^n(f)$ . Hence  $\text{im } H^n(f) \subset \ker H^n(g)$ .

For the reverse inclusion, let  $[b] \in \ker H^n(g) \subset H^n(B)$ . Then  $g(b) \in C^n$  must be a coboundary, so that there is some  $c \in C^{n-1}$  such that  $g(b) = d_C c$ . Choose a lift  $b_1 \in B^{n-1}$  of  $c$ , meaning that  $g(b_1) = c$ . Then  $b - d_B b_1 \in Z^n(B)$ , and  $[b] = [b - d_B b_1]$ . But

$$g(b - d_B b_1) = g(b) - g(d_B b_1) = g(b) - d_C g(b_1) = g(b) - d_C c = 0.$$

Hence  $b - d_B b_1 \in \ker g \subset B^n$ . This implies that there exists a unique  $a \in A^n$  such that  $b - d_B b_1 = f(a)$ . Also,

$$f(d_A a) = d_B(f(a)) = d_B(b - d_B b_1) = 0.$$

Since  $f$  is injective, we see that  $d_A a = 0$ , i.e.,  $a \in Z^n(A)$ . Thus,  $H^n(f)([a]) = [f(a)] = [b - d_B b_1] = [b]$ . This proves that  $[b] \in \text{im } H^n(f)$ .

Exactness at  $H^n(C)$ : Let  $[b] \in H^n(B)$ . Note that  $\delta^n(H^n(g)([b])) = [a]$  where  $a \in A^{n+1}$  denotes the unique element such that  $f(a) = d_B b$ . Since  $d_B b = 0$  and  $f$  is injective, it follows that  $a = 0$ . Hence  $\text{im } H^n(g) \subset \ker \delta^n$ .

Conversely, let  $[c] \in \ker \delta^n$ . Choose  $b \in B^n$  such that  $g(b) = c$  and then the unique  $a \in A^{n+1}$  such that  $f(a) = d_B b$ . Thus,  $\delta^n([c]) = [a] = 0$ , so that  $a \in B^{n+1}(A)$ , i.e.,  $d_A a_1 = a$  for some  $a_1 \in A^n$ . Note that  $g(b - f(a_1)) = g(b) - g(f(a_1)) = c - 0 = c$ . Further,

$$\begin{aligned} d_B(b - f(a_1)) &= d_B(b) - d_B(f(a_1)) \\ &= f(a) - f(d_A a_1) \\ &= f(a) - f(a) \\ &= 0. \end{aligned}$$

This shows that  $b - f(a_1)$  is a cocycle. Thus,  $H^n(g)([b - f(a_1)]) = [g(b - f(a_1))] = [c]$ , so that  $[c] \in \text{im } H^n(g)$ .

Exactness at  $H^{n+1}(A)$ : Let  $[c] \in H^n(C)$  and find  $[a] = \delta^n([c])$ , where

$$\begin{array}{ccc} & b & \xrightarrow{g} c \\ & \downarrow & \\ a & \xrightarrow{f} & d_B b \end{array}.$$

Then  $H^{n+1}(f)([a]) = [f(a)] = [d_B b] = 0$ . It follows that  $\text{im } \delta^n \subset \ker H^{n+1}(f)$ .

Conversely, let  $[a] \in \ker H^{n+1}(f)$ , so that  $H^{n+1}(f)([a]) = [f(a)] = 0$ . This means that  $f(a) = d_B b$  for some  $b \in B^n$ . Then  $\delta^n([g(b)]) = [a]$ . This shows that  $\text{im } \delta^n \supset \ker H^{n+1}(f)$ .  $\square$

## 12 Additive categories

**Definition 12.0.1.**

1. A category  $\mathcal{C}$  is *enhanced over  $\mathbf{Ab}$*  if  $\text{Hom}_{\mathcal{C}}(a, b)$  is an abelian group for any  $a, b \in \text{ob } \mathcal{C}$  and

$$\text{Hom}_{\mathcal{C}}(y, z) \times \text{Hom}_{\mathcal{C}}(x, y) \xrightarrow{\circ} \text{Hom}_{\mathcal{C}}(x, z)$$

is bilinear for any  $x, y, z \in \text{ob } \mathcal{C}$ .

2. A category  $\mathcal{C}$  is called *additive* if it is enhanced over  $\mathbf{Ab}$  and has finite products.

**Example 12.0.2.** The following are additive categories.

1.  $\mathbf{Ab}$ .
2.  $R\text{-Mod}$ .

**Note 12.0.3.**

1. Let  $\mathcal{C}$  be category with finite products. The product of the empty diagram is the terminal object in  $\mathcal{C}$  since it is the initial object in  $\mathbf{Set}$ .
2. If  $\mathcal{C}$  is additive and  $*$  is the terminal object in  $\mathcal{C}$ , then  $\text{Hom}_{\mathcal{C}}(*, *)$  consists of a single element, which must equal the group identity element.

**Exercise 12.0.4.** Verify the following statements.

1. If  $\mathcal{C}$  is a additive, then its terminal object is also initial and thus is a zero object in  $\mathcal{C}$ .
2. A zero object  $0_{\mathcal{C}}$  satisfies  $\text{Hom}_{\mathcal{C}}(x, 0_{\mathcal{C}}) = 0$  and  $\text{Hom}_{\mathcal{C}}(0_{\mathcal{C}}, x) = 0$  for any  $x \in \text{ob } \mathcal{C}$ .
3. Any additive category has finite coproducts that are equal to finite products.

## 12.1 Lecture 26

**Definition 12.1.1.** Let  $\mathcal{C}$  be an additive category. Let  $f : x \rightarrow y$  be a morphism in  $\mathcal{C}$ .

1. A *kernel (object)* for  $f$  is a pair  $(k, q)$  where  $k \in \text{ob } \mathcal{C}$  and  $q : k \rightarrow x$  such that for any  $z \in \text{ob } \mathcal{C}$ , the natural sequence

$$\text{Hom}(z, k) \xrightarrow{q \circ -} \text{Hom}(z, x) \xrightarrow{f \circ -} \text{Hom}(z, y)$$

is exact.

2. A *cokernel (object)* for  $f$  is a pair  $(c, p)$  where  $c \in \text{ob } \mathcal{C}$  and  $p : y \rightarrow c$  such that for any  $z \in \text{ob } \mathcal{C}$ , the natural sequence

$$\text{Hom}(c, z) \xrightarrow{- \circ p} \text{Hom}(y, z) \xrightarrow{- \circ f} \text{Hom}(x, z)$$

is exact.

**Definition 12.1.2.** We say that a category  $\mathcal{A}$  is *abelian* if

1.  $\mathcal{A}$  is additive and
2. for any morphism  $f : x \rightarrow y$  in  $\mathcal{A}$ , there exists a sequence  $k \xrightarrow{q} x \xrightarrow{a} i \xrightarrow{b} y \xrightarrow{p} c$  in  $\mathcal{A}$  such that
  - (a)  $(k, q)$  is a kernel for  $f$ ,
  - (b)  $(c, p)$  is a cokernel for  $f$ ,
  - (c)  $(c, a)$  is a cokernel for  $q$ , and
  - (d)  $(i, b)$  is a kernel for  $p$ .

We call  $i$  the *image* of  $f$ .

**Definition 12.1.3.** If  $\mathcal{A}$  is an abelian, then a sequence  $x \xrightarrow{f} y \xrightarrow{g} z$  in  $\mathcal{A}$  is *exact* if  $\text{im } f = \ker g$ .

**Example 12.1.4.**

1. **Ab.**
2.  **$R\text{-Mod}$ .**
3.  **$\text{PreShAb}_X$**  where  $X$  is a space.

*Remark 12.1.5.* Our notion of and results for cohomology for complexes of abelian groups hold for complexes of objects in an abelian category.

**Theorem 12.1.6 (Freyd-Mitchell).** *Every abelian category admits a fully faithful embedding into  $R\text{-Mod}$  for some ring  $R$ .*

*Remark 12.1.7.* It is not, in general, possible to complete an additive category  $\mathcal{C}$  to an abelian one. Still, we can always add enough images to  $\mathcal{C}$  to get cones of maps of complexes.

Let  $\mathcal{C}$  be additive. A map  $e : x \rightarrow x$  in  $\mathcal{C}$  is an *idempotent* if  $e^2 = e$ . Let  $\mathcal{C} = \mathbf{Vect}_k$ . Then an idempotent map  $e : x \rightarrow x$  is a projection map, i.e.,  $x = x_1 \oplus x_2$  such that  $e = i_1 \circ p_1$ .

If  $\mathcal{C}$  is additive and  $e : x \rightarrow x$  is idempotent in  $\mathcal{C}$ , then we say that  $e$  *has an image in  $\mathcal{C}$*  if there exists a decomposition  $x = x_1 \oplus x_2$  such that

$$e = \begin{bmatrix} \text{id}_{x_1} & 0 \\ 0 & 0 \end{bmatrix}$$

with respect to this decomposition. We say that  $x_1$  is the *image of  $e$* .

Let  $e : x \rightarrow x$  be an idempotent. Then  $\text{id}_x e : x \rightarrow x$  is also an idempotent. Indeed,

$$(\text{id}_x - e)^2 = \text{id}_x^2 - \text{id}_x e - e \text{id}_x + e^2 = \text{id}_x - e = e.$$

If  $x = x_1 \oplus x_2$  has  $e = \begin{bmatrix} \text{id}_{x_1} & 0 \\ 0 & 0 \end{bmatrix}$ , then  $\text{id}_x - e = \begin{bmatrix} 0 & 0 \\ 0 & \text{id}_{x_2} \end{bmatrix}$ , so that  $\text{id}_x - e$  has  $x_2$  as an image.

**Definition 12.1.8.** A category  $\mathcal{C}$  is *idempotent complete* or *Karoubian* if  $\mathcal{C}$  is additive and any idempotent in  $\mathcal{C}$  has an image in  $\mathcal{C}$ .

**Exercise 12.1.9.** Show that for any additive category  $\mathcal{C}$ , there exists a unique (up to unique isomorphism) category  $\mathcal{C}^{\text{Kor}}$  together with a functor  $F : \mathcal{C} \rightarrow \mathcal{C}^{\text{Kor}}$  such that

1.  $\mathcal{C}^{\text{Kor}}$  is idempotent complete,
2.  $F$  is fully faithful, and
3. every object in  $\mathcal{C}^{\text{Kor}}$  is an image of an idempotent in  $\mathcal{C}$ .

**Definition 12.1.10.** A *graded additive category* is an additive category  $\mathcal{C}$  such that for any  $x, y \in \text{ob } \mathcal{C}$ ,  $\text{Hom}(x, y)$  is a graded abelian group, i.e.,  $\text{Hom}(x, y) \cong \bigoplus_{n \in \mathbb{Z}} \text{Hom}^n(x, y)$  and  $\text{Hom}(x, y) \times \text{Hom}(y, z) \xrightarrow{\circ} \text{Hom}(x, z)$  has the form  $\text{Hom}^n(x, y) \times \text{Hom}^m(y, z) \xrightarrow{\circ} \text{Hom}^{n+m}(x, z)$  where  $\circ$  is bilinear.

**Definition 12.1.11.** A graded additive category  $\mathcal{C}$  is a *differential graded category* if for any  $x, y \in \text{ob } \mathcal{C}$ , the graded group  $\text{Hom}(x, y)$  is equipped with with a homomorphism  $d : \text{Hom}(x, y) \rightarrow \text{Hom}(x, y)$  such that

- (a)  $d : \text{Hom}^n(x, y) \rightarrow \text{Hom}^{n+1}(x, y)$ ,
- (b)  $d^2 = 0$ , and
- (c)  $d$  satisfies the *graded Leibniz rule*, i.e., if  $f \in \text{Hom}^n(x, y)$  and  $g \in \text{Hom}(a, x)$ , then

$$d(f \circ g) = df \circ g + (-1)^n f \circ dg.$$

**Proposition 12.1.12.** Let  $\mathcal{C}$  be a category.

1. If  $\mathcal{C}$  is additive, then for any  $x \in \text{ob } \mathcal{C}$ ,  $\text{Hom}(x, x)$  is a ring (in fact, a  $\mathbb{Z}$ -algebra).

2. If  $\mathcal{C}$  is a graded additive category, then for any  $x \in \text{ob } \mathcal{C}$ ,  $\text{End}(x)$  is a graded ring.
3. If  $\mathcal{C}$  is differential graded category, then for any  $x \in \text{ob } \mathcal{C}$ ,  $\text{End}(x)$  is a differential graded algebra.

**Definition 12.1.13.** If  $\mathcal{C}$  is a differential graded category, then the *homotopy category* of  $\mathcal{C}$  is the category  $\text{Ho}(\mathcal{C})$  (or  $[\mathcal{C}]$ ) given by

$$\begin{aligned} \text{ob } \text{Ho}(\mathcal{C}) &\equiv \text{ob } \mathcal{C} \\ \text{Hom}_{\text{Ho}(\mathcal{C})}(x, y) &\equiv H^0(\text{Hom}_{\mathcal{C}}(x, y), d) \\ &= \frac{\ker(\text{Hom}_{\mathcal{C}}^0(x, y) \xrightarrow{d} \text{Hom}_{\mathcal{C}}^1(x, y))}{\text{im}(\text{Hom}_{\mathcal{C}}^{-1}(x, y) \xrightarrow{d} \text{Hom}_{\mathcal{C}}^0(x, y))}. \end{aligned}$$

Let  $\mathcal{B}$  be an additive category. Define the category  $\mathbf{Compl}(\mathcal{B})$  of complexes in  $\mathcal{B}$  by

$$\begin{aligned} \text{ob } \mathbf{Compl}(\mathcal{B}) &= (\text{complexes of objects in } \mathcal{B}) \\ \text{mor } \mathbf{Compl}(\mathcal{B}) &= (\text{morphisms of complexes}). \end{aligned}$$

This is an additive category. We can also refine this definition by incorporating degree-shifting maps to get a differential graded category of complexes in  $\mathcal{B}$ . Define the category  $\mathbf{Compl}^\bullet(\mathcal{B})$  by

$$\begin{aligned} \text{ob } \mathbf{Compl}^\bullet(\mathcal{B}) &= (\text{complexes of objects in } \mathcal{B}) \\ \text{Hom}_{\mathbf{Compl}^\bullet(\mathcal{B})}(M, N) &= \bigoplus_{n \in \mathbb{Z}} \text{Hom}^n(M, N) \end{aligned}$$

where

$$\text{Hom}^n(M, N) \equiv \prod_{a \in \mathbb{Z}} \text{Hom}_{\mathcal{B}}(M^a, N^{a+n}).$$

The composition is obtained component-wise from the composition in  $\mathcal{B}$ . Define  $d : \text{Hom}^n(M, N) \rightarrow \text{Hom}^{n+1}(M, N)$  by

$$(f_a)_{a \in \mathbb{Z}} \rightarrow (d_N \circ f_a + (-1)^n f_{a+1} \circ d_M)_{a \in \mathbb{Z}}.$$

This makes  $\mathbf{Compl}^\bullet(\mathcal{B})$  a differential graded category.

Let  $M, N \in \text{ob } \mathbf{Compl}^\bullet(\mathcal{B})$ . Then

$$\begin{aligned} Z^0(\text{Hom}_{\mathbf{Compl}^\bullet(\mathcal{B})}(M, N)) &= \ker(\text{Hom}^0 \xrightarrow{d} \text{Hom}^1) \\ &= \text{Hom}_{\mathbf{Compl}(\mathcal{B})}(M, N) \\ B^0(\text{Hom}_{\mathbf{Compl}^\bullet(\mathcal{B})}(M, N)) &= \text{im}(\text{Hom}^{-1} \xrightarrow{d} \text{Hom}^0) \\ &= (\text{homotopies of 0-maps of complexes}). \end{aligned}$$

Also, we have that

$$H^0(\text{Hom}_{\mathbf{Compl}^\bullet(\mathcal{B})}(M, N)) = (\text{maps of complexes}) / (\text{homotopies}).$$

**Example 12.1.14.**  $\text{Ho}(\mathbf{Comp}^\bullet(\mathbf{Ab})) = \mathcal{C}(\mathbf{Ab})$ , and  $Z^0(\mathbf{Comp}^\bullet(\mathbf{Ab})) = \mathbf{CoCh}(\mathbf{Ab})$ .

## 13 Triangulated categories

### 13.1 Lecture 27

Let  $\mathcal{C}$  be a category. For any  $x \in \text{ob } \mathcal{C}$ , define  $x[n]$  as the object, if it exists, in  $\mathcal{C}$  that represents the shift functor on morphisms  $\text{Hom}_{\mathcal{C}}(-, x)[n] : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Compl}(\mathbf{Ab})$ . If  $f : x \rightarrow y$  is a morphism in  $\mathcal{C}$ , then define the *cone*  $\text{cone}(f)$  of  $f$  to be the object, if it exists, in  $\mathcal{C}$  that represents the functor  $\mathcal{C}^{\text{op}} \rightarrow \mathbf{Compl}(\mathbf{Ab})$  given by  $z \mapsto \text{cone}(\text{Hom}_{\mathcal{C}}(z, x) \xrightarrow{f \circ -} \text{Hom}_{\mathcal{C}}(z, y))$ .

**Definition 13.1.1.** A category  $\mathcal{C}$  is called *strongly pre-triangulated* if every object in  $\mathcal{C}$  has shifts in  $\mathcal{C}$  and every morphism in  $\mathcal{C}$  has cones in  $\mathcal{C}$ . We call  $\mathcal{C}$  *pre-triangulated* if every object in  $\mathcal{C}$  has shifts in  $\text{Ho}(\mathcal{C})$  and every morphism in  $\mathcal{C}$  has cones in  $\text{Ho}(\mathcal{C})$ .

**Note 13.1.2.** Both the assignment  $x \mapsto x[n]$  and the assignment  $f \mapsto \text{cone}(f)$  are functorial.

**Definition 13.1.3.** Given a differential graded category  $\mathcal{C}$ , we define  $\text{Ho}^{\bullet}(\mathcal{C})$  as the graded additive category such that

$$\begin{aligned} \text{ob } \text{Ho}^{\bullet}(\mathcal{C}) &= \text{ob } \mathcal{C} \\ \text{Hom}_{\text{Ho}^{\bullet}(\mathcal{C})}(x, y) &= H^{\bullet}(\text{Hom}_{\mathcal{C}}(x, y)). \end{aligned}$$

If  $\mathcal{C}$  is strongly pre-triangulated, then  $\text{Ho}^{\bullet}(\mathcal{C})$  and  $\text{Ho}(\mathcal{C})$  contain the same information. Indeed,  $\text{Ho}(\mathcal{C})$  is precisely the degree zero piece of  $\text{Ho}^{\bullet}(\mathcal{C})$ . Conversely, if  $x, y \in \text{ob } \mathcal{C}$ , then

$$\text{Hom}_{\text{Ho}^{\bullet}(\mathcal{C})}(x, y) = \bigoplus_{a \in \mathbb{Z}} \text{Hom}_{\text{Ho}^{\bullet}(\mathcal{C})}^a(x, y)$$

where  $\text{Hom}_{\text{Ho}^{\bullet}(\mathcal{C})}^a(x, y) = \text{Hom}_{\text{Ho}(\mathcal{C})}(x, y[a]) = \text{Hom}_{\text{Ho}(\mathcal{C})}(x, y)[a]$ .

*Notation.* From now on, if  $\mathcal{C}$  is strongly pre-triangulated, then we write  $\text{Ho}(\mathcal{C})$  for the graded homotopy category.

**Definition 13.1.4.** If  $\mathcal{C}$  is strongly pre-triangulated, then a *triangle*  $\triangle$  in  $\text{Ho}(\mathcal{C})$  is a sequence of degree zero maps  $x \xrightarrow{u} y \xrightarrow{v} z \xrightarrow{w} x[1]$ . We represent this as

$$\begin{array}{ccc} x & \xrightarrow{u} & y \\ & \nwarrow w & \downarrow v \\ & & z \end{array}.$$

Let  $\mathcal{C}$  be strongly pre-triangulated. Given a triangle

$$\begin{array}{ccc} x & \xrightarrow{u} & y \\ & \nwarrow w & \downarrow v \\ & & z \end{array},$$



we have a long sequence of maps

$$\begin{array}{ccccccc}
 x[-1] & \xrightarrow{u[-1]} & y[-1] & \xrightarrow{v[-1]} & z[-1] & & \\
 & & \searrow w[-1] & & & & \\
 x & \xleftarrow{u} & y & \xrightarrow{v} & z & & \\
 & & \nwarrow w & & & & \\
 x[1] & \xleftarrow{u[1]} & y[1] & \xrightarrow{v[1]} & z[1] & \xrightarrow{w[1]} & \cdots
 \end{array}$$

in  $\mathcal{C}$ .

**Definition 13.1.5.** Let  $\mathcal{C}$  be strongly pre-triangulated. We say that a triangle in  $\text{Ho}(\mathcal{C})$  is *exact* if it is isomorphic to the triangle

$$x \xrightarrow{u} y \xrightarrow{\text{"inclusion"}} \text{cone}(u) \xrightarrow{\text{"projection''}} x[1] .$$

**Definition 13.1.6.** A graded additive category  $\mathcal{D}$  is *triangulated* if  $\mathcal{D}$  is equipped with a shift functor  $[1] : \mathcal{D} \rightarrow \mathcal{D}$  and a collection of *distinguished triangles* such that the following axioms hold.

- (0) Every triangle that is isomorphic to a distinguished triangle is distinguished.
- (1) For any object  $x$  in  $\mathcal{D}$ , the triangle  $x \xrightarrow{\text{id}_x} x \rightarrow 0 \rightarrow x[1]$  is distinguished.
- (2) (*rotation invariance*) The shift rotation of a triangle  $\triangle$  is distinguished if and only if  $\triangle$  is, i.e., the triangle  $x \xrightarrow{u} y \xrightarrow{v} z \xrightarrow{w} x[1]$  is distinguished if and only if the triangle

$$y \xrightarrow{v} z \xrightarrow{w} x[1] \xrightarrow{-u[1]} y[1]$$

is distinguished.

- (3) Every morphism  $u : x \rightarrow y$  can be included in a distinguished triangle  $x \xrightarrow{u} y \xrightarrow{v} z \xrightarrow{w} x[1]$ , and every commutative square

$$\begin{array}{ccc}
 x & \xrightarrow{u} & y \\
 f \downarrow & & \downarrow g \\
 x' & \xrightarrow{u'} & y'
 \end{array}$$

can be completed to a commutative diagram of distinguished triangles, i.e.,

$$\begin{array}{ccccccc}
 x & \xrightarrow{u} & y & \xrightarrow{v} & z & \xrightarrow{w} & x[1] \\
 f \downarrow & & \downarrow g & & \downarrow h & & \downarrow f[1] \\
 x' & \xrightarrow{u'} & y' & \xrightarrow{v'} & z' & \xrightarrow{w'} & x'[1]
 \end{array}$$

- (4) (*octahedron axiom*) Given any two distinguished triangles  $x \xrightarrow{u} y \xrightarrow{v} z \xrightarrow{w} x[1]$  and  $y \xrightarrow{f} z \xrightarrow{g} w \xrightarrow{h} y[1]$

$y' \xrightarrow{g} q \xrightarrow{h} y[1]$ , we can complete them to a commutative diagram

$$\begin{array}{ccccccc}
 x & \xrightarrow{u} & y & \xrightarrow{v} & z & \xrightarrow{w} & x[1] \\
 \parallel & & \downarrow f & & \downarrow a & & \parallel \\
 x & \longrightarrow & y' & \longrightarrow & z' & \longrightarrow & x[1] \\
 & & \downarrow g & & \downarrow b & & \downarrow u[1] \\
 & & q & \xlongequal{\quad} & q & \longrightarrow & y[1] \\
 & & \downarrow h & & \downarrow c & & \\
 & & y[1] & \longrightarrow & z[1] & & 
 \end{array}$$

where each new triangle is distinguished.

The octahedron axiom is the formal transplant of the second isomorphism theorem for  $\mathbf{Comp}(\mathbf{Ab})$ ,<sup>1</sup> which states that given two complexes  $L$  and  $M$ , an inclusion  $f : L \hookrightarrow M$ , and a subcomplex  $N$  of  $L$  and of  $M$ , we have that  $M/L \cong (M/N)/(L/N)$ , i.e., if

$$\begin{array}{ccccccc}
 & & N & & N & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & M/L \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L/N & \longrightarrow & M/N & \longrightarrow & (M/N)/(L/N) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

has exact rows and exact left two columns, then the third column is also exact.

Now, suppose that  $\mathcal{C}$  is strongly pre-triangulated and let  $\alpha : M \rightarrow N$  be a morphism in  $\mathcal{C}$  such that  $\alpha$  is injective (i.e.,  $\ker \alpha$  exists and is trivial) with  $d\alpha = 0$  and  $\alpha$  is split (i.e., there exists  $\beta : N \rightarrow M$  with  $\beta \circ \alpha = \text{id}_M$ ). We call such an  $\alpha$  a *split monomorphism* in  $\mathcal{C}$ .

**Lemma 13.1.7.**

- (i) The map  $\text{cone}(\alpha) \rightarrow N/M$  is a homotopy equivalence.
- (ii) Any morphism in  $\mathcal{C}$  is homotopy equivalent to a split mono, i.e., given  $f : M \rightarrow L$ , we can construct a natural diagram

$$\begin{array}{ccc}
 M & \xrightarrow{\alpha} & N \\
 & \searrow f & \downarrow g \\
 & & L
 \end{array}$$

in  $\mathcal{C}$  such that  $\alpha$  is a split mono and  $g$  is an iso in  $\text{Ho}(\mathcal{C})$ .

*Partial proof.* For (ii), take  $N = L \oplus \text{cone}(\text{id}_M)$ . □

<sup>1</sup>The second isomorphism theorem holds in some form for any abelian category.

**Theorem 13.1.8.** *If  $\mathcal{C}$  is a strongly pre-triangulated differential graded category and  $\mathcal{D} = \text{Ho}(\mathcal{C})$ , then  $\mathcal{D}$  is triangulated with exact triangles as the distinguished triangles.*

*Proof.*

Verifying axioms (0) and (1) is trivial.

For axiom (2), if  $x \rightarrow y \rightarrow z \rightarrow x[1]$  is a triangle, then we can use Lemma 13.1.7 to rewrite it as a homotopy equivalent triangle  $M \rightarrow N \rightarrow L \rightarrow M[1]$  where  $M \xrightarrow{\alpha} N$  is a split mono. In this case, we can check that  $N \rightarrow L \rightarrow M[1] \rightarrow N[1]$  is exact by using the splitting.

For axiom (3), note that any  $u : x \rightarrow y$  is included in  $x \rightarrow y \rightarrow \text{cone}(u) \rightarrow x[1]$ . Moreover, if

$$\begin{array}{ccc} x & \xrightarrow{u} & y \\ f \downarrow & & \downarrow g \\ x' & \xrightarrow{u'} & y' \end{array}$$

is commutative in  $\text{Ho}(\mathcal{C})$  and we lift  $f, g, u$ , and  $u'$  to maps  $\tilde{\cdot}$  in  $\mathcal{C}$ , then we get a diagram

$$\begin{array}{ccccccc} x & \xrightarrow{\tilde{u}} & y & \longrightarrow & \text{cone}(u) & \longrightarrow & x[1] \\ \tilde{f} \downarrow & & \downarrow \tilde{g} & & M \downarrow & & \downarrow \tilde{f}[1] \\ x' & \xrightarrow{\tilde{u}'} & y' & \longrightarrow & \text{cone}(u') & \longrightarrow & x'[1] \end{array}$$

in  $\mathcal{C}$  where  $M \equiv \begin{bmatrix} \delta & 0 \\ 0 & 0 \end{bmatrix}$ ,  $\delta \in \text{Hom}^{-1}(x, y')$ , and  $\tilde{g} \circ \tilde{u} - \underbrace{\tilde{u}' \circ \tilde{f}}_{d(\delta)} \sim 0$ .

For axiom (4), given a distinguished triangle  $M \rightarrow N \rightarrow L \rightarrow M[1]$ , we apply Lemma 13.1.7 twice to get a homotopy equivalent distinguished triangle  $M \rightarrow N' \rightarrow L'' \rightarrow M[1]$  where each map in this is a split mono. We are done after an application of the second isomorphism theorem.  $\square$

*Remark 13.1.9.* Such reasoning can be applied to complete any differential graded category to a triangulated one.

## 13.2 Lecture 28

**Definition 13.2.1.** If  $\mathcal{A}$  and  $\mathcal{B}$  are differential graded categories, then a *differential graded functor*  $F : \mathcal{A} \rightarrow \mathcal{B}$  has the following properties.

- (i)  $F$  is additive, i.e.,  $F : \text{Hom}_{\mathcal{A}}(x, y) \rightarrow \text{Hom}_{\mathcal{B}}(F(x), F(y))$  is a group homomorphism for any  $x, y \in \text{ob } \mathcal{A}$ .
- (ii)  $F$  respects differentials, i.e., if  $x, y \in \text{ob } \mathcal{A}$ , then  $F : \text{Hom}_{\mathcal{A}}(x, y) \rightarrow \text{Hom}_{\mathcal{B}}(F(x), F(y))$  is a map of complexes.

If  $F, G : \mathcal{A} \rightarrow \mathcal{B}$  are two differential graded functors between differential graded categories, then define, for each  $n \in \mathbb{Z}$ , the group

$$\text{Hom}^n(F, G) \equiv \{ \varphi_x \mid \varphi_x : F(x) \rightarrow G(x) \text{ in } \text{Hom}_{\mathcal{B}}^n(F(x), G(x)), x \in \text{ob } \mathcal{A} \}.$$

A map  $F \rightarrow G$  is defined as a natural transformation  $F \rightarrow G$  such that each component  $\varphi_x : F(x) \rightarrow G(x)$  belongs to  $\text{Hom}_{\mathcal{B}}^n(F(x), G(x))$ . The differential on  $\prod_{x \in \text{ob } \mathcal{A}} \text{Hom}^\bullet(F(x), G(x))$  induces a differential on

$$\text{Hom}^\bullet(F, G) \equiv \bigoplus_{n \in \mathbb{Z}} \text{Hom}^n(F, G).$$

This produces a complex of maps between  $F$  and  $G$ , and we get a differential graded category  $\mathbf{dgFun}(\mathcal{A}, \mathcal{B})$ .

**Exercise 13.2.2.** *Prove the following assertions.*

1. If  $F : \mathcal{A} \rightarrow \mathcal{B}$  is a differential graded functor, then  $H^0(F) : H^0(\mathcal{A}) \rightarrow H^0(\mathcal{B})$  is an additive functor.
2. If  $F, G : \mathcal{A} \rightarrow \mathcal{B}$  are differential graded functors, then there is an embedding  $H^0(\text{Hom}(F, G)) \subset \text{Hom}(H^0(F), H^0(G))$ .

**Definition 13.2.3.** If  $\mathcal{A}$  is a differential graded category, then a *left  $\mathcal{A}$ -module* is a differential graded functor  $\mathcal{A} \rightarrow \mathbf{Compl}(\mathbf{Ab})$  and a *right  $\mathcal{A}$ -module* is a differential graded functor  $\mathcal{A}^{\text{op}} \rightarrow \mathbf{Compl}(\mathbf{Ab})$ .

If  $\mathcal{A}$  is a differential graded category with a single object  $*$ , then  $\mathcal{A} \leftrightarrow R := \text{Hom}_{\mathcal{A}}(*, *)$ , which is precisely the complex of abelian groups equipped with a multiplication-like operation  $\cdot$  such that  $\lambda$  satisfies the graded Leibniz rule for  $\cdot$ .

**Exercise 13.2.4.** *Show that a module over  $\mathcal{A}$  is precisely the data of a complex  $x$  of abelian groups together with a differential graded algebra homomorphism  $R \rightarrow \text{Hom}_{\mathbf{Compl}(\mathbf{Ab})}(x, x)$ .*

Given a differential graded category  $\mathcal{A}$ , we have respective categories of left and right modules over  $\mathcal{A}$  that are linear over a field  $k$ , namely

$$\begin{aligned} \mathcal{A}\text{-dgmod}_k &\equiv \mathbf{dgFun}(\mathcal{A}, \mathbf{Compl}(k\text{-Vect})) \\ \text{dgmod}_k\text{-}\mathcal{A} &\equiv \mathbf{dgFun}(\mathcal{A}^{\text{op}}, \mathbf{Compl}(k\text{-Vect})). \end{aligned}$$

**Exercise 13.2.5.** *Show that the functors*

$$\begin{aligned} h^\bullet : \mathcal{A}^{\text{op}} &\rightarrow \mathcal{A}\text{-dgmod}_k \\ x &\mapsto h^\times \equiv \text{Hom}_{\mathcal{A}}(x, -) \\ h_\bullet : \mathcal{A} &\rightarrow \text{dgmod}_k\text{-}\mathcal{A} \\ h_\times &\equiv \text{Hom}_{\mathcal{A}^{\text{op}}}(x, -) = \text{Hom}_{\mathcal{A}}(-, x) \end{aligned}$$

*are fully faithful differential graded functors.*

**Proposition 13.2.6.**

1. If  $\mathcal{A}$  is a small differential graded category, then  $H^0(\mathcal{A}^{\text{op}}\text{-dgmod}_k)$  is triangulated.

2. If  $\mathcal{A}$  is a pre-triangulated differential graded category, then the fully faithful functor

$$H^0(h_\bullet) : H^0(\mathcal{A}) \rightarrow H^0(\mathcal{A}^{\text{op}}\text{-}\mathbf{dgmod}_k)$$

gives a triangulated structure on  $H^0(\mathcal{A})$ .

**Definition 13.2.7.** We say that an object  $F$  in  $\mathcal{A}^{\text{op}}\text{-}\mathbf{dgmod}_k$  is *compact* or *perfect* if  $F : \mathcal{A}^{\text{op}} \rightarrow \mathbf{Compl}(k\text{-}\mathbf{Vect})$  commutes with arbitrary coproducts.

**Note 13.2.8.**  $h^\times$  is compact for any  $x \in \text{ob } \mathcal{A}$ .

**Definition 13.2.9.** We say that a  $k$ -linear differential graded category  $\mathcal{A}$  is *triangulated* if every compact object in  $\mathcal{A}^{\text{op}}\text{-}\mathbf{dgmod}_k$  is representable.

**Note 13.2.10.** A triangulated differential graded category is automatically strongly pre-triangulated, and  $H^0(\mathcal{A})$  is triangulated.

**Exercise 13.2.11.**

1. Suppose that  $\mathcal{D}$  is a triangulated additive category. Let  $M \rightarrow N \rightarrow C \rightarrow M[1]$  be a distinguished triangle. Show that for every  $L \in \text{ob } \mathcal{D}$ , the sequence

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \text{Hom}(L, M) & \longrightarrow & \text{Hom}(L, N) & \longrightarrow & \text{Hom}(L, C) \\ & & & & & \swarrow & \\ & & & & & \text{Hom}(L, M[1]) & \longrightarrow \text{Hom}(L, N[1]) \longrightarrow \text{Hom}(L, C[1]) \longrightarrow \cdots \end{array}$$

is a long exact sequence of abelian groups.

2. Suppose that  $\mathcal{D}$  is triangulated. Show that the sum  $\Delta_1 \oplus \Delta_2$  of two triangles in  $\mathcal{D}$  is distinguished if and only if both  $\Delta_1$  and  $\Delta_2$  are distinguished.

**Definition 13.2.12.** If  $\mathcal{D}_1$  and  $\mathcal{D}_2$  are triangulated additive categories, then a *triangulated* (or *exact*) functor  $F : \mathcal{D}_1 \rightarrow \mathcal{D}_2$  is an additive functor such that

- (i)  $F$  is equipped with an isomorphism  $\sigma : F \circ [1] \rightarrow [1] \circ F$  and
- (ii)  $F$  sends distinguished triangles to distinguished triangles.

A *morphism of two triangulated functors*  $(F, \theta_F)$  and  $(G, \theta_G)$  is a morphism  $f : F \rightarrow G$  of additive functors such that  $f$  intertwines  $\theta_F$  and  $\theta_G$ . As a result, we have a category of triangulated functors  $\mathcal{D}_1 \rightarrow \mathcal{D}_2$ .

If  $\mathcal{A}$  and  $\mathcal{B}$  are differential graded categories and  $F : \mathcal{A} \rightarrow \mathcal{B}$  is a differential graded functor, then we have a natural differential graded functor  $\mathcal{A}^{\text{op}}\text{-}\mathbf{dgmod}_k \xrightarrow{F} \mathcal{B}^{\text{op}}\text{-}\mathbf{dgmod}_k$  so that  $H^0(F)$  is triangulated.

**Definition 13.2.13.** If  $\mathcal{D}$  is a triangulated category and  $\mathcal{A}$  is an abelian category, then a *cohomological functor* is a functor  $H : \mathcal{D} \rightarrow \mathcal{A}$  such that

- (i)  $H$  is additive and
- (ii)  $H$  sends distinguished  $\Delta$ 's in  $\mathcal{D}$  into long exact sequences in  $\mathcal{A}$ .

**Example 13.2.14.**

1. If  $\mathcal{C}(\mathbf{Ab})$  denotes the triangulated category of homotopy classes of complexes of abelian groups, then  $H^\bullet : \mathcal{C}(\mathbf{Ab}) \rightarrow \mathbf{grAb}$  is a cohomological functor.
2. If  $\mathcal{D}$  is a triangulated category and  $L \in \text{ob } \mathcal{D}$ , then  $h^L : \mathcal{D} \rightarrow \mathbf{Ab}$  given by  $M \mapsto Z^0(\text{Hom}_{\mathcal{D}}(L, M))$  is a cohomological functor.

### 13.3 Lecture 29

Let  $\mathcal{D}$  be a triangulated category and  $\mathcal{V} \subset \mathcal{D}$  a triangulated subcategory (i.e., the inclusion functor is triangulated). We wish to construct a quotient category  $\mathcal{D}/\mathcal{V}$ , i.e., a triangulated category  $\mathcal{D}/\mathcal{V}$  together with a triangulated functor  $q : \mathcal{D} \rightarrow \mathcal{D}/\mathcal{V}$  such that

- $q(x) = 0$  for any  $x \in \text{ob } \mathcal{V}$  and
- for any triangulated functor  $f : \mathcal{D} \rightarrow \mathcal{D}'$  satisfying  $x \in \text{ob } \mathcal{V} \implies f(x) = 0$ , we have  $g \circ q = f$ .

**Note 13.3.1.**

1. In the triangulated category of triangulated categories with exact functors, the triangle  $\mathcal{V} \rightarrow \mathcal{D} \rightarrow \mathcal{D}/\mathcal{V} \rightarrow \mathcal{V}[1]$  is exact.
2. If  $\mathcal{D}$  is triangulated and  $u : x \rightarrow y$  is a morphism in  $\mathcal{D}$ , then there exists an object  $\text{cone}(u)$  in  $\mathcal{D}$  that is unique up to a non-unique isomorphism. This is the third term in a distinguished  $\Delta$  completing  $u$ .

**Exercise 13.3.2.** Show that if  $u : x \rightarrow y$  is a map in  $\mathcal{D}$ , then it is an isomorphism in  $\mathcal{D}$  if and only if  $\text{cone}(u) = 0$ .

**Definition 13.3.3.** If  $\mathcal{D}$  is a triangulated category and  $\mathcal{V} \subset \mathcal{D}$  a triangulated subcategory, then a morphism  $u : x \rightarrow y$  in  $\mathcal{D}$  is a  $\mathcal{V}$ -quasi-isomorphism if  $\text{cone}(u) \in \text{ob}(\mathcal{V})$ .

**Exercise 13.3.4.** Let  $\mathcal{V} \subset \mathcal{D}$  be a pair of triangulated categories. Use the octahedron axiom to show that if  $f$  and  $g$  are compassable morphisms in  $\mathcal{D}$ , then every morphism in  $\{f, g, g \circ f\}$  is a  $\mathcal{V}$ -quasi-isomorphism if and only if at least two morphisms in it are  $\mathcal{V}$ -quasi-isomorphisms.

*Remark 13.3.5.* One may define  $\mathcal{D}/\mathcal{V}$  as the localization of  $\mathcal{D}$  in the set of all  $\mathcal{V}$ -quasi-isomorphisms. But doing so requires a lot of work.

**Definition 13.3.6.** Suppose that  $\mathcal{I}$  is a small category. We say that  $\mathcal{I}$  is a *directed category* if it satisfies the following properties.

(1) If  $x_1, x_2 \in \text{ob } \mathcal{J}$ , then there is some diagram

$$\begin{array}{ccc} x_1 & \longrightarrow & x_3 \\ & \nearrow & \\ x_2 & & \end{array}$$

of maps in  $\mathcal{J}$ .

(2) If

$$\begin{array}{ccc} x_1 & \longrightarrow & x_2 \\ & \searrow & \\ & & x_3 \end{array}$$

is a diagram of maps in  $\mathcal{J}$ , then there exist maps  $x_2 \rightarrow x_4; x_3 \rightarrow x_4$  in  $\mathcal{J}$  such that

$$\begin{array}{ccccc} x_1 & \longrightarrow & x_2 & \longrightarrow & x_4 \\ & \searrow & & \nearrow & \\ & & x_3 & & \end{array}$$

commutes in  $\mathcal{J}$ .

(3) For any two parallel maps  $f, g : x \rightarrow y$ , there exists a map  $h : y \rightarrow z$  such that  $h \circ f = h \circ g$ .

Let  $\mathcal{J}$  be small. There is a well-defined functor  $\text{colim} : \text{Fun}(\mathcal{J}, \mathbf{Ab}) \rightarrow \mathbf{Ab}$ , but this need *not* be exact even though both  $\mathbf{Ab}$  and  $\text{Fun}(\mathcal{J}, \mathbf{Ab})$  are abelian.

**Exercise 13.3.7.** *Show, however, that if  $\mathcal{J}$  is directed, then  $\text{colim}$  is an exact functor.*

Now, let  $\mathcal{V} \subset \mathcal{D}$  be a pair of triangulated categories. Let  $x \in \text{ob } \mathcal{D}$  and let  $\mathcal{Q}/x$  be the full subcategory of  $\mathcal{D}/x$  consisting of morphisms  $y \rightarrow x$  that are  $\mathcal{V}$ -quasi-isomorphisms. Similarly, let  $x/\mathcal{Q}$  be the full subcategory of  $x/\mathcal{D}$  consisting morphisms  $x \rightarrow z$  that are  $\mathcal{V}$ -quasi-isomorphisms.

**Exercise 13.3.8.** *Prove the following assertions.*

1. Both  $x/\mathcal{Q}$  and  $(\mathcal{Q}/x)^{\text{op}}$  are directed categories.
2. Any map in  $x/\mathcal{Q}$  or  $\mathcal{Q}/x$  is automatically a  $\mathcal{V}$ -quasi-isomorphism.

**Definition 13.3.9.** Define the *Verdier quotient of  $\mathcal{D}$  by  $\mathcal{V}$*  as the category  $\mathcal{D}/\mathcal{V}$  with  $\text{ob } \mathcal{D}/\mathcal{V} \equiv \text{ob } \mathcal{D}$  and  $\text{Hom}_{\mathcal{D}/\mathcal{V}}(a, b) \equiv \text{colim}_{a' \in (\mathcal{Q}/a)^{\text{op}}} \text{Hom}_{\mathcal{D}}(a', b)$ .

There exists a canonical isomorphism

$$\text{colim}_{a' \in (\mathcal{Q}/a)^{\text{op}}} \text{Hom}_{\mathcal{D}}(a', b) \cong \text{colim}_{b' \in (b/\mathcal{Q})} \text{Hom}_{\mathcal{D}}(a, b').$$

For this, we must check that given a top triangle

$$\begin{array}{ccc} a' & \xrightarrow{\text{q-iso}} & a \\ & \searrow & \downarrow \\ & & b \end{array},$$

we can form a commutative double triangle

$$\begin{array}{ccccc} a' & \xrightarrow{\text{q-iso}} & a & \longrightarrow & b' \\ & \searrow & \downarrow & \nearrow & \\ & & b & & \end{array} \quad .$$

As a result, we get  $q : \mathcal{D} \rightarrow \mathcal{D}/\mathcal{V}$ .

**Lemma 13.3.10.** *If  $x \in \text{ob } \mathcal{D}$  has  $q(x) = 0$  in  $\mathcal{D}/\mathcal{V}$ , then  $x$  is a direct summand of an object in  $\mathcal{V}$ .*

*Proof.* We have that  $q(x) = 0 \iff$  there is some  $y \in \mathcal{D}$  such that  $\varphi : y \rightarrow x$  is a  $\mathcal{V}$ -quasi-isomorphism. In this case,  $\underbrace{\text{cone}(\varphi)}_{y[1] \oplus x} \in \mathcal{V}$ .  $\square$

**Definition 13.3.11.** A triangulated subcategory  $\mathcal{V} \subset \mathcal{D}$  is *thick* if any object in  $\mathcal{D}$  that is isomorphic to a direct summand of an object in  $\mathcal{V}$  is an object in  $\mathcal{V}$ .

**Note 13.3.12.** If  $\mathcal{V}$  is a strict full thick triangulated subcategory of  $\mathcal{D}$ , then  $q : \mathcal{D} \rightarrow \mathcal{D}/\mathcal{V}$  kills all and only objects in  $\mathcal{V}$ .

**Definition 13.3.13.** If  $\mathcal{D}$  is triangulated and  $\mathcal{U}, \mathcal{V} \subset \mathcal{D}$  are strict full triangulated subcategories, then  $(\mathcal{U}, \mathcal{V})$  is an *admissible pair of subcategories* if

- (a)  $\text{Hom}_{\mathcal{D}}(x, y) = 0$  for any  $x \in \text{ob } \mathcal{U}$  and  $y \in \text{ob } \mathcal{V}$  and
- (b) any object  $z \in \text{ob } \mathcal{D}$  fits in a distinguished triangle  $x \rightarrow z \rightarrow y \rightarrow x[1]$  with  $x \in \text{ob } \mathcal{U}$  and  $y \in \text{ob } \mathcal{V}$ .

**Exercise 13.3.14.** *Prove the following assertions.*

1. The  $\triangle$  in condition (b) is unique up to a unique isomorphism and is functorial in  $z$ .
2. The functor  $\mathcal{D} \rightarrow \mathcal{U}$  given by  $z \mapsto x(z)$  is triangulated and is right adjoint to  $\mathcal{U} \hookrightarrow \mathcal{D}$ .  
Dually, the functor  $\mathcal{D} \rightarrow \mathcal{V}$  given by  $z \mapsto y(z)$  is triangulated and is left adjoint to  $\mathcal{V} \hookrightarrow \mathcal{D}$ .
3. Each of  $\mathcal{U}$  and  $\mathcal{V}$  determines the other. Specifically,

$$\begin{aligned} \mathcal{V} &= \mathcal{U}^\perp \equiv \underbrace{\{y \in \text{ob } \mathcal{D} \mid \text{Hom}_{\mathcal{D}}(x, y) = 0, \ x \in \text{ob } \mathcal{U}\}}_{\text{full subcategory}} \\ \mathcal{U} &= {}^\perp \mathcal{V} \equiv \underbrace{\{x \in \text{ob } \mathcal{D} \mid \text{Hom}_{\mathcal{D}}(x, y) = 0, \ y \in \text{ob } \mathcal{V}\}}_{\text{full subcategory}}. \end{aligned}$$

In particular, both  $\mathcal{U}$  and  $\mathcal{V}$  are thick subcategories.

4. The natural compositions  $\mathcal{U} \hookrightarrow \mathcal{D} \rightarrow \mathcal{D}/\mathcal{V}$  and  $\mathcal{V} \hookrightarrow \mathcal{D} \rightarrow \mathcal{D}/\mathcal{U}$  are triangulated equivalences.

**Definition 13.3.15.** An additive pair  $(\mathcal{U}, \mathcal{V})$  is called a *semiorthogonal decomposition* of  $\mathcal{D}$  into  $\mathcal{U}$  and  $\mathcal{V}$ .



**Proposition 13.3.16.** *If  $\mathcal{U} \subset \mathcal{D}$  is a strict full triangulated thick subcategory, then TFAE.*

1. *The inclusion  $\mathcal{U} \hookrightarrow \mathcal{D}$  has a left adjoint.*
2. *The quotient  $\mathcal{D} \rightarrow \mathcal{D}/\mathcal{U}$  has a right adjoint.*
3.  *$(\mathcal{U}, \mathcal{U}^\perp)$  is admissible.*

**Definition 13.3.17.** If  $\mathcal{A}$  is an abelian category, then the *derived category of  $\mathcal{A}$*  is the triangulated category

$$\mathcal{D}(\mathcal{A}) \equiv \mathcal{C}(\mathcal{A}) / \mathcal{C}(\mathcal{A})^{\text{acyclic}},$$

where  $\mathcal{C}(\mathcal{A})^{\text{acyclic}}$  is the full subcategory of  $\mathcal{C}(\mathcal{A})$  consisting of those  $x$  with zero cohomology.

To do computations in  $\mathcal{D}(\mathcal{A})$ , we must understand when  $\mathcal{D}(a)$  can be embedded in  $\mathcal{C}(\mathcal{A})$  so that  $(\mathcal{C}(\mathcal{A})^{\text{acyclic}}, \mathcal{D}(\mathcal{A}))$  is an adjoint pair. This requires  $(\mathcal{C}(\mathcal{A})^{\text{acyclic}})^\perp$  to be large.

Define  ${}^\perp\mathcal{C}(\mathcal{A})^{\text{acyclic}}$  as the category of *homotopically projective objects* in  $\mathcal{C}(\mathcal{A})$  and  $(\mathcal{C}(\mathcal{A})^{\text{acyclic}})^\perp$  as the category of *homotopically injective objects* in  $\mathcal{C}(\mathcal{A})$ .

**Proposition 13.3.18.**

1. *Every bounded-above complex of projectives is a homotopically projective object in  $\mathcal{C}(\mathcal{A})$ .*
2. *Any bounded-below complex of injectives is a homotopically injective object in  $\mathcal{C}(\mathcal{A})$ .*