

Introduction to Commutative Algebra

Vítězslav Kala

English AI translation by Claude Opus 5

September 24, 2026

Contents

1	Basics	5
1.1	Introduction	5
1.2	Ideals and factor rings	5
1.3	Prime ideals and maximal ideals	7
1.4	Principal ideals and divisibility	8
1.5	Noetherianity	9
1.6	Irreducible polynomials	11
1.7	Chinese remainder theorem	13
1.8	Zorn's lemma	15
2	Galois theory	17
2.1	Review	17
2.2	Introduction	17
2.3	Integral elements	18
2.4	Root fields and splitting fields	19
2.5	Algebraic closure	21
2.6	The Galois group	24
2.7	Separable extensions	24
2.8	Simple extensions	27
2.9	Normal extensions	29
2.10	Galois correspondence	30
2.11	Computations of Galois groups	33
3	Algebraic geometry	34
3.1	Algebraic sets and ideals	34
3.2	Radicals	37
3.3	Finitely generated fields	38
3.4	Hilbert's Nullstellensatz	40
3.5	Irreducible algebraic sets	41
4	Algebraic number theory	43
4.1	Factorizations of Diophantine equations	43
4.1.1	$x^2 + 1 = y^3$	43
4.1.2	$x^2 + 5 = y^3$	43
4.2	Integral elements	45
4.3	Norm and trace	46
4.4	Ideals	47
4.5	Cancellation of ideals	49
4.6	The norm of an ideal	50
4.7	Prime ideals and factorization	51
4.8	Description of prime ideals	52

4.9	Examples in $K = \mathbb{Q}(\sqrt{-14})$	55
5	Exercise sheets	56
5.1	Exercises 1	56
5.2	Exercises 2	57
5.3	Exercises 3	58
5.4	Exercises 4	59
5.5	Exercises 5	60
5.6	Exercises 6	61
5.7	Exercises 7	62
6	Solutions to the exercises	64
6.1	Exercises 1	64
6.2	Exercises 2	67
6.3	Exercises 3	70
6.4	Exercises 4	74
6.5	Exercises 5	77
6.6	Exercises 6	82
6.7	Exercises 7	87
7	Homework assignments	94
7.1	Homework 1	94
7.2	Homework 2	94
7.3	Homework 3	94

Introduction

This is a working version of the lecture notes for the course Introduction to Commutative Algebra; hopefully it no longer contains too many typos and imperfections – but I will be glad for any remarks and comments.

Their aim is to be a fairly minimalist summary of the material covered (in the scope taught from 2017 onwards), which closely follows the course of the lectures and contains almost no additional information.

The material in these notes and its presentation is not original at all: Chapters 1 and 2 are based on the lecture notes of Aleš Drápal [Dr] and partly of David Stanovský [St], Chapter 3 on the book by William Fulton [Fu] and Chapter 4 on the text of Keith Conrad [Co].

Chapters 5, 6 and 7 summarize the exercise sessions and homework assignments, partly following the teaching in 2019/2020; they were later written down and completed by Matěj Doležálek.

The lectures in 2019/2020 were recorded and are available here:

<https://is.mff.cuni.cz/prednasky/prednaska/NMAG301/>

I thank Jakub Novák for writing down the notes; the exercises, and in particular their solutions in Chapter 6, were written by Matěj Doležálek. For pointing out mistakes and typos I thank the students who took the course in the winter semester 2019/2020 (and also in the following years). For further corrections I thank David Stanovský and Claude Opus 5.5. Despite our efforts, the current version undoubtedly contains a number of mistakes, typos and unclear passages, so I will welcome any comments and suggestions for improvement. In time, perhaps at least a few explanatory and motivating comments will be added.

This is an AI translation primarily done by Claude Opus 5. It hasn't been human-checked, so use at your own risk! The Czech original is available at <https://karlin.mff.cuni.cz/~kala/files/UKA26.pdf>

[Co] Keith Conrad, *Factoring in quadratic fields*

<http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/quadraticgrad.pdf>

[Dr] Aleš Drápal, *Komutativní okruhy* [Commutative rings]

<http://www.karlin.mff.cuni.cz/~zemlicka/11-12/komalg.pdf>

[Fu] William Fulton, *Algebraic curves*

<http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf>

[St] David Stanovský, *Základy algebry* [Foundations of algebra], the chapter on Galois theory

http://www.karlin.mff.cuni.cz/~stanovsk/vyuka/alg_galois.pdf

1. Basics

1.1 Introduction

Notation:

In these notes we use the following notation, which is rather unusual at MFF.

- $A \subset B$ denotes non-strict inclusion, i.e. $A = B$ is allowed. Strict inclusion is denoted $A \subsetneq B$
- The invertible elements of a ring are denoted $R^\times$ instead of R^*
- We do not use the notation $\mathbb{Z}_n$; instead we write $\mathbb{Z}/n = \mathbb{Z}/(n)$ (which one can think of as the set $\{0, 1, \dots, n-1\}$ with the operations taken modulo n)
- $(\mathbb{Z}/(n))^\times$ = the numbers coprime to n , modulo n
- the size of a set M is denoted $\#M$
- $A \twoheadrightarrow B$ denotes a surjection (and often a surjective homomorphism)
- $A \hookrightarrow B$ denotes an embedding (and often an injective homomorphism)

1.2 Ideals and factor rings

By a ring we mean $R(+, -, 0, \cdot)$, where both $+$ and $\cdot$ are commutative.

Except in this section, we always assume that rings always have 1.

Let R be a ring. An ideal I is a non-empty subset of R such that:

- $a, b \in I \Rightarrow a + b, a - b \in I$
- $a \in I, r \in R \Rightarrow ra \in I$

Ideals are denoted $I < R$.

Usually the definition also includes the condition $0 \in I$: but it follows from the other two. Similarly, if $1 \in R$, then also $-1 \in R$, and hence $-b \in I$ (2nd condition), so that $a - b \in I$ follows from the 1st condition.

Definition. Define the relation $a \sim b \Leftrightarrow a - b \in I$ (sometimes written $a \equiv b \pmod{I}$). It is an equivalence.

The classes are denoted $[a] = a + I := \{a + i \mid i \in I\}$

Indeed, if $b \in [a]$, then $b - a \in I$ (by def.), hence $b \in a + I = \{a + i \mid i \in I\}$.

Definition. The set of equivalence classes modulo an ideal I is the *factor ring* and is denoted R/I .

On the classes we define $+, \cdot$

$$(a + I) + (b + I) := (a + b) + I$$

$$(a + I) \cdot (b + I) := (a \cdot b) + I$$

$$0_{R/I} = 0 + I, 1_{R/I} = 1 + I, -(a + I) = (-a) + I$$

Example. $R = \mathbb{Z}, I = 6\mathbb{Z} = \{\dots, -6, 0, 6, 12, \dots\}$

$a \sim b \Leftrightarrow a - b \in 6\mathbb{Z} \Leftrightarrow a \equiv b \pmod{6}$

Classes:

$0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, \dots, 5 + 6\mathbb{Z}$

$R/I = \mathbb{Z}/6\mathbb{Z}$ has 6 elements: it is the usual $\mathbb{Z}/6$

Example. R a ring, I, J ideals in R such that $J \subset I$

a) Then J is an ideal in I . (I is a ring, typically without 1)

Let us check: Closedness of J under addition and subtraction: OK (because it is an ideal in R).

Closedness of J under multiplication by elements of I : OK (because $I \subset R$ and J is an ideal in R)

b) I/J is an ideal in R/J .

Let us check:

$R/J = \{a + J \mid a \in R\}$

$I/J = \{i + J \mid i \in I\} \subset R/J$

I/J closed under $+$:

Let $a + J, b + J \in I/J$.

Then $a \in I, b \in I$, and hence $a + b \in I$.

Thus $(a + J) + (b + J) = (a + b) + J \in I/J$.

(Subtraction completely analogously.)

I/J closed under $\cdot$ by elements of R/J , i.e.:

If $a + J \in I/J, r + J \in R/J$, then I want $(a + J)(r + J) = ar + J \in I/J$ (EXERCISE)

$\varphi: R \rightarrow S$ a ring homomorphism.

$R \supset \text{Ker } \varphi = \{r \in R \mid \varphi(r) = 0\}$

$\text{Im } \varphi = \{\varphi(r) \mid r \in R\} \subset S$

Theorem 1.1 (Homomorphism theorem). *Let $\varphi: R \rightarrow S$ be a ring homomorphism and $I \subset R$ an ideal such that $I \subset \text{Ker } \varphi$. Then*

$$\begin{aligned} \psi: R/I &\rightarrow S \\ a + I &\mapsto \varphi(a) \end{aligned}$$

is a well-defined ring homomorphism. Moreover, $\text{Ker } \psi = \text{Ker } \varphi / I$ and $\text{Im } \psi = \text{Im } \varphi$.

Proof. 1) Well defined: Let $a + I = b + I$, i.e. $b = a + i, i \in I$. Then $\psi(b + I) = \varphi(b) = \varphi(a) + \varphi(i) \stackrel{i \in \text{Ker } \varphi}{=} \varphi(a) + 0 = \varphi(a) = \psi(a + I)$.

2) Homomorphism: We need to check that it preserves $+, \cdot$ (and $-$ in the case of a ring without 1): Let $(a + I)(b + I) = ab + I$. Then $\psi((a + I)(b + I)) = \psi(ab + I) = \varphi(ab) \stackrel{\varphi \text{ hom.}}{=} \varphi(a)\varphi(b) = \psi(a + I)\psi(b + I)$. $+, -$ are checked similarly.

3) Im is clear.

I is an ideal in $\text{Ker } \varphi, \psi(a + I) = 0 \Leftrightarrow \varphi(a) = 0$. Hence

$\text{Ker } \varphi / I = \{a + I \mid a \in \text{Ker } \varphi\} = \text{Ker } \psi$. □

Theorem 1.2 (1st isomorphism theorem). *Let $\varphi: R \rightarrow S$ be a (ring) homomorphism. Then*

$$R/\text{Ker } \varphi \simeq \text{Im } \varphi, \quad a + \text{Ker } \varphi \mapsto \varphi(a).$$

Proof. In the homomorphism theorem 1.1 choose $I = \text{Ker } \varphi$. We get a homomorphism $\psi: R/\text{Ker } \varphi \rightarrow S$.

Its image is $\text{Im } \psi = \text{Im } \varphi$, and hence $\psi: R/\text{Ker } \varphi \twoheadrightarrow \text{Im } \varphi$.

Is ψ injective? A homomorphism is injective if $\psi(\alpha) = 0 \Leftrightarrow \alpha = 0$. So let $\alpha = a + \text{Ker } \varphi$. $0 = \psi(a + \text{Ker } \varphi) = \varphi(a) \Rightarrow a \in \text{Ker } \varphi \Rightarrow a + \text{Ker } \varphi = \text{Ker } \varphi = [0]$. $\square$

Theorem 1.3 (2nd isomorphism theorem). *R a ring, I, J ideals such that $J \subset I$. Then $J < I, I/J < R/J$ and $(R/J)/(I/J) \simeq R/I$.*

Proof. Consider the projection

$$\begin{aligned} \varphi: R &\twoheadrightarrow R/I, \\ a &\mapsto a + I. \end{aligned}$$

Clearly it is surjective and $\text{Ker } \varphi = I$.

By the homomorphism theorem 1.1 for φ and $J \subset R$ (which we may use, because $J < \text{Ker } \varphi = I$), we have $\exists \psi: R/J \rightarrow R/I$. Moreover $\text{Im } \psi = \text{Im } \varphi = R/I, \text{Ker } \psi = \text{Ker } \varphi/J = I/J$. Hence by Theorem 1.2 we have $(R/J)/\text{Ker } \psi \simeq \text{Im } \psi$. $\square$

Corollary 1.4. *Let R be a ring and J an ideal. The ideals in R/J are exactly the I/J , where I is an ideal in R such that $J \subset I$.*

Proof. We know that $I/J < R/J$ thanks to the example above.

Conversely, let I_0 be an ideal in R/J . We want to prove that $I_0 = I/J$ for some I . The elements of I_0 are of the form $a + J$, so it makes sense to define $I := \{a \in R \mid a + J \in I_0\}$; clearly $J \subset I$.

We want:

1) I is an ideal in R :

Let $a, b \in I, r \in R$. Then $a + J, b + J \in I_0$, hence $a + b + J \in I_0$, i.e. $a + b \in I$. The same for $ra \in I$.

2) $I/J = I_0$:

Writing it out by means of the definition of I we have

$$I/J = \{i + J \mid i \in I\} = \{a + J \mid a \in R, a + J \in I_0\} = I_0. \quad \square$$

Theorem 1.5 (3rd isomorphism theorem). *R a ring, $I < R$ an ideal, $S \subset R$ a subring. Then $S + I = \{s + a \mid s \in S, a \in I\}$ is a subring in R and $(S + I)/I \simeq S/(S \cap I)$*

Proof. EXERCISE. (The projection $\pi: R \twoheadrightarrow R/I$ and its restriction to $\varphi: S \rightarrow R/I$. The 1st isomorphism theorem for φ .) $\square$

1.3 Prime ideals and maximal ideals

Recall that from now until the end of the notes all rings have 1 (and are commutative).

Definition. R a ring. $I < R$ is a proper ideal if $I \neq R$.

A proper ideal I is maximal if there is no proper ideal $J < R$ such that $I \subsetneq J$.

For ideals I, J we define $IJ = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N} \right\}$.

A proper ideal P is a prime ideal if for all ideals $I, J < R$ we have $IJ \subset P \Rightarrow I \subset P$ or $J \subset P$.

An ideal I is principal if $\exists a \in R$ such that $I = (a) = aR$.

Example. $R = \mathbb{Z}$. All ideals in $\mathbb{Z}$ are of the form $I = (n) = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}$, where $n = 0, 1, 2, \dots$.

Clearly $(n) = (-n)$.

Divisibility of numbers $2 \mid 6$ corresponds to the reverse inclusion of ideals $(2) \supset (6)$.

So if $I = (a)$, $J = (b)$ and $P = (p)$, then we have:

$$IJ = (ab)$$

$$(p) \supset (ab) \Leftrightarrow p \mid ab$$

$$(p) \supset (a) \Leftrightarrow p \mid a$$

$$(p) \supset (b) \Leftrightarrow p \mid b$$

Hence $P = (p)$ is a prime ideal $\Leftrightarrow |p|$ is a prime number or $p = 0$.

$5\mathbb{Z}$ is a prime ideal, but $10\mathbb{Z}$ is not, because $(2) \cdot (5) \subset (10)$, but $(2) \not\subset (10)$ and $(5) \not\subset (10)$.

Lemma 1.6. *A proper ideal I in a ring R is a prime ideal if and only if for any two elements $a, b \in R$ we have $ab \in I \Rightarrow a \in I$ or $b \in I$.*

Proof. “ $\Rightarrow$ ” Let I be a prime ideal and let $ab \in I$. Then $(aR)(bR) = (abR) \subset I$. By the definition we thus have $aR \subset I$ or $bR \subset I$, and hence $a \in I$ or $b \in I$.

“ $\Leftarrow$ ” Let J_1, J_2 be ideals such that $J_1 J_2 \subset I$. Assume that $J_2 \not\subset I$, i.e. that there is $b \in J_2 \setminus I$. For every $a \in J_1$ we have $ab \in J_1 J_2 \subset I$, and hence $a \in I$ or $b \in I$. But $b \notin I$, and hence $a \in I$ for every $a \in J_1$. It follows that $J_1 \subset I$, as we wanted. $\square$

Definition. S is an (integral) domain if $\forall a, b \in S$ we have $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Observation. An element a is invertible $\Leftrightarrow (a) = aR = R$.

A ring R is a field $\Leftrightarrow (0)$ is its only proper ideal.

Corollary 1.7. *Let I be a proper ideal in R . Then:*

a) I is maximal $\Leftrightarrow R/I$ is a field

b) I is a prime ideal $\Leftrightarrow R/I$ is a domain.

Proof. a)

“ $\Rightarrow$ ” I maximal $\Rightarrow$ the only proper ideal of the ring R which lies between R and I is I itself.

Corollary 1.4 $\Rightarrow$ the ideals of R/I are exactly the J/I , where $J \supset I$. Hence only $J = R$ or $J = I$ is possible. But these correspond to the improper ideal $R/I < R/I$ and $I/I = (0_{R/I}) < R/I$.

Observation $\Rightarrow R/I$ is a field.

“ $\Leftarrow$ ” Similarly, R/I a field $\Rightarrow (0_{R/I})$ is the only proper ideal in R/I .

Corollary 1.4 $\Rightarrow$ the only proper ideals in R which contain I are I and $R \Rightarrow I$ is maximal.

b)

“ $\Rightarrow$ ” I a prime ideal. Let $a + I, b + I \in R/I$ be such that $ab + I = (a + I)(b + I) = 0_{R/I} = I$. Then $ab \in I$. By Lemma 1.6 we then have $a \in I \Rightarrow a + I = I = 0_{R/I}$ or $b \in I \Rightarrow b + I = 0_{R/I}$, i.e. we have verified the definition of a domain.

“ $\Leftarrow$ ” Let R/I be a domain and $ab \in I$. We want (by Lemma 1.6) that $a \in I$ or $b \in I$.

$ab \in I \Rightarrow I = ab + I = (a + I)(b + I) \xrightarrow{R/I \text{ domain}} a + I = I$ or $b + I = I \Rightarrow a \in I$ or $b \in I$. $\square$

1.4 Principal ideals and divisibility

Definition. Let R be a ring.

$$a \mid b \Leftrightarrow \exists c : b = ac$$

$$a \parallel b \Leftrightarrow a \mid b \text{ and } b \mid a$$

Observation. $a \mid b \Leftrightarrow (a) \supset (b), a \parallel b \Leftrightarrow (a) = (b)$

Definition. A domain R is Gaussian if every $a \in R, a \neq 0$, has a unique factorization into a product of irreducible elements, i.e. $a \parallel p_1^{k_1} \cdots p_n^{k_n}$, where $n \geq 0, k_i \geq 1$ and p_i are irreducible elements such that $p_i \nparallel p_j$ for $i \neq j$.

Remark (A theorem from Algebra). Let R be a domain. Then R is Gaussian if and only if:

1. a gcd of all pairs of elements exists and
2. there is no sequence of elements $a_1, a_2, \dots \in R$ such that $a_{i+1} \mid a_i$ and $a_{i+1} \nparallel a_i$.

Example. $\mathbb{Z}, \mathbb{Q}[x], \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$ are Gaussian, because they are Euclidean.

$\mathbb{Z}[x]$ is Gaussian, but not Euclidean.

$\mathbb{Z}[\sqrt{D}]$ for $D < 0$ almost never is: it is Gaussian if and only if $D = -1, -2$.

$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ for $D < 0$ is Gaussian if and only if $D = -3, -7, -11, -19, -43, -67, -163$.

Whether $\mathbb{Z}[\sqrt{D}]$ for $D > 0$ is Gaussian for infinitely many D is a famous open problem; it is expected that the answer is yes.

Definition. A domain R is a principal ideal domain (PID) if every ideal is principal, i.e. $\forall I \subset R, \exists a \in R : I = (a)$.

Definition. $I + J = \{a + b \mid a \in I, b \in J\}$

Proposition 1.8. Let R be a PID. Then R is Gaussian and Bézout's identity holds: $\forall a, b \in R \exists r, s \in R : \gcd(a, b) = ar + bs$.

Proof. We verify the two conditions from the remark above:

1) Existence of gcd: For $a, b \in R$ consider the ideal $(a) + (b)$. We are in a PID $\Rightarrow \exists c : (a) + (b) = (c)$. We have $(a) \subset (c) \Rightarrow c \mid a$ and $(b) \subset (c) \Rightarrow c \mid b$.

If d is a common divisor of a, b , then $(a) \subset (d), (b) \subset (d) \Rightarrow (c) = (a) + (b) \subset (d) \Rightarrow d \mid c$. Hence c is the *greatest* common divisor. Bézout's identity follows from $(a) + (b) = (c)$.

2) By contradiction, let us have $\dots a_{i+1} \mid a_i \mid a_{i-1} \mid \dots \mid a_1$ with $a_{i+1} \nparallel a_i$ for all i . Then $(a_1) \subsetneq (a_2) \subsetneq \dots \subsetneq (a_i) \subsetneq \dots$ is a chain of principal ideals. Consider $I = \bigcup_{i=1}^{\infty} (a_i)$, which is an ideal (exercise).

PID $\Rightarrow \exists a \in R : I = (a)$.

$a \in \bigcup_{i=1}^{\infty} (a_i) \Rightarrow \exists i : a \in (a_i)$. Then $(a) \subset (a_i) \subsetneq (a_{i+1}) \subset \bigcup_{i=1}^{\infty} (a_i) = (a)$. Contradiction. $\square$

1.5 Noetherianity

Definition. A ring R is Noetherian if it contains no infinite increasing chain of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$

For example, a field is always Noetherian (because it contains only two ideals).

The definition resembles $\dots \mid a_3 \mid a_2 \mid a_1 \Rightarrow (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$

Proposition 1.9. Principal ideal domains are Noetherian.

Proof. Let R be a PID. Suppose it is not Noetherian. Then there is $I_1 \subsetneq I_2 \subsetneq \dots$. Consider $I := \bigcup_{j=1}^{\infty} I_j$,

which is an ideal (exercise). PID $\Rightarrow I$ is principal, $I = (a)$.

$a \in I = \bigcup I_j \Rightarrow \exists j : a \in I_j$. We have $I_j \subset I_{j+1} \Rightarrow a \in I_{j+1} \Rightarrow (a) \subset I_j \subset I_{j+1} \subset I = (a) \Rightarrow$ equalities everywhere $\Rightarrow I_j = I_{j+1}$. Contradiction. $\square$

$$\text{Euclidean} \Rightarrow \text{PID} \Rightarrow \begin{cases} \text{Gaussian} \\ \text{Noetherian} \end{cases}$$

$\mathbb{Z}[\sqrt{-2019}]$ is Noetherian, but not Gaussian.

$R = K[X, Y]$ is Gaussian, Noetherian, not a PID.

$R = K[X_1, X_2, X_3, \dots]$ is Gaussian, but *not* Noetherian.

Definition. Let R be a ring. An R -module M is an abelian group $M(+, -, 0)$ together with a scalar multiplication $r \cdot m \in M$ for $r \in R, m \in M$ such that $\forall r, s \in R, \forall m, n \in M$:

- $r(m + n) = rm + rn$
- $r(sm) = (rs)m$
- $(r + s)m = rm + sm$
- $1m = m$

It is a notion similar to a vector space, but over a ring.

If R is a field, then an R -module is the same thing as an R -vector space.

Example.

- Every abelian group G is a $\mathbb{Z}$ -module.
 $im = m + m + \dots + m, i \in \mathbb{N}, m \in G$
 $(-i) \cdot m = -(im)$
- R is an R -module
- $I < R \Rightarrow I$ is an R -module

Definition. An R -module M is Noetherian if there is no infinite sequence $M_1 \subsetneq M_2 \subsetneq \dots$ of R -submodules in M .

Observation. A ring R is a Noetherian ring $\Leftrightarrow R$ is a Noetherian R -module.

Definition. Let M be an R -module and $X \subset M$ its subset. The set of all finite sums $\sum_{i=1}^k r_i x_i$, for $r_i \in R, x_i \in X$ is the smallest R -submodule in M which contains X . It is called the submodule generated by X .

If there is a *finite* set X which generates M , then M is a finitely generated R -module.

Definition. Let us have elements $r_1, \dots, r_k$ in a ring R . The ideal generated by them is denoted $(r_1, \dots, r_k) = r_1 R + \dots + r_k R$ (it is at the same time the smallest ideal which contains the given elements).

Proposition 1.10. An R -module M is Noetherian $\Leftrightarrow$ every R -submodule $N \subset M$ is finitely generated.

Proof.

“ $\Leftarrow$ ” By contradiction: Let us have a sequence $M_1 \subsetneq M_2 \subsetneq \dots$

Then $N = \bigcup_{i=1}^{\infty} M_i$ is an R -module $\Rightarrow N$ is finitely generated by some elements $n_1, n_2, \dots, n_k$. $N =$

$\bigcup M_i \Rightarrow \exists j$ such that $n_1, \dots, n_k \in M_j$

$\Rightarrow$ the R -module generated by $n_1, \dots, n_k$ is a subset of $M_j \Rightarrow N \subset M_j$.

So we have $N \subset M_j \subsetneq M_{j+1} \subset N$. Contradiction.

“ $\Rightarrow$ ” By contradiction: Let $N \subset M$ be an R -submodule which is not finitely generated.

Let $M_0 = \{0\}$. Successively choose $m_i \in N \setminus M_i$ and define $M_{i+1} := M_i + R \cdot m_i$, which is possible, because M_i is finitely generated and N is not finitely generated, hence $M_i \subsetneq N$. (Strictly speaking, to ensure the existence of this sequence we need the axiom of choice.)

We have produced an infinite sequence $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots$, which is a contradiction. $\square$

Theorem 1.11 (Hilbert's basis theorem). *A ring R is Noetherian if and only if $R[x]$ is Noetherian.*

Proof. “ $\Leftarrow$ ” exercise.

“ $\Rightarrow$ ” Let R be Noetherian and $R[x]$ not. By Proposition 1.10 there then exists an $R[x]$ -submodule in $R[x]$ which is not finitely generated, i.e. there is an ideal $I < R[x]$ which is not finitely generated. Let $f_0 \in I$ be a nonzero polynomial of the smallest degree and f_{i+1} some polynomial of the smallest degree in $I \setminus (f_0, f_1, \dots, f_i)$. Clearly $\deg f_0 \leq \deg f_1 \leq \dots$.

Let a_i be the leading coefficient of the polynomial f_i and J_i = the ideal in R generated by the elements $a_0, \dots, a_i$. $J_0 \subset J_1 \subset J_2 \dots$ is a chain in the Noetherian ring $R \Rightarrow \exists k: J_k = J_{k+1} = J_{k+2} = \dots$.

In particular $\exists r_0, \dots, r_k \in R: a_{k+1} = r_0 a_0 + \dots + r_k a_k$.

Let $d = \deg f_{k+1}$; we can multiply the polynomials $f_0, f_1, \dots, f_k$ by suitable $x^{\text{something}}$ so that we obtain polynomials $\tilde{f}_0, \dots, \tilde{f}_k$, all of degree d . Consider $g := f_{k+1} - r_0 \tilde{f}_0 - \dots - r_k \tilde{f}_k$. Then we have $\deg g \leq d$, but the coefficient of x^d is $a_{k+1} - r_0 a_0 - \dots - r_k a_k = 0 \Rightarrow \deg g < d = \deg f_{k+1}$.

But $g \in I \setminus (f_0, \dots, f_k)$, which contradicts the choice of f_{k+1} of the smallest degree. $\square$

Corollary 1.12. *If R is Noetherian, then $R[x_1, \dots, x_k]$ is also Noetherian.*

1.6 Irreducible polynomials

Throughout this section: R is a Gaussian domain and T its field of fractions.

For $a \in R$ let $a \parallel p_1^{k_1} \dots p_n^{k_n}$ be its factorization into prime factors, $p_i \nmid p_j$, for $i \neq j$, $k_i \geq 1$, $n \geq 0$. Then $(a) = (p_1)^{k_1} \dots (p_n)^{k_n}$, because $(b) \cdot (c) = (bc)$ (exercise).

Exercise: p is a prime factor $\Leftrightarrow (p)$ is a prime ideal.

Definition. Let p be a prime factor. Then the p -valuation of an element $a \in R$ is

- $v_p(a) = \begin{cases} k_i & \text{if } \exists i: p \parallel p_i (\Leftrightarrow (p) = (p_i)) \\ 0 & \text{otherwise.} \end{cases}$
- $v_p(0) = \infty$.

For $t = \frac{a}{b} \in T$ we define $v_p(t) := v_p(a) - v_p(b)$.

Clearly we have $v_p(uv) = v_p(u) + v_p(v)$, and hence $v_p(t)$ is well defined, because $v_p(\frac{ca}{cb}) = v_p(ca) - v_p(cb) = v_p(a) - v_p(b) = v_p(\frac{a}{b})$.

Definition. Let $f(x) = \sum_{i=0}^d a_i x^i \in T[x]$ and $p \in R$ a prime factor.

The p -content of the polynomial f is $c_p(f) = \min\{v_p(a_i), 0 \leq i \leq d\}$.

For a polynomial $f \in R[x]$ we say that it is primitive if $\gcd(a_0, \dots, a_d) = 1$, i.e. $c_p(f) = 0$ for all irreducible elements $p \in R$.

Lemma 1.13.

- a) Let $u \in T^\times = T \setminus \{0\}$, p a prime factor in R and $f \in T[x] \setminus \{0\}$. Then $c_p(u \cdot f) = c_p(f) + v_p(u)$.
- b) Let $a \in T$. Then $a \in R$ if and only if $v_p(a) \geq 0$ for all irreducible elements $p \in R$.
- c) Let $f \in T[x]$. Then $f \in R[x]$ if and only if $c_p(f) \geq 0$ for all irreducible elements $p \in R$.

Proof. a) We have $v_p(ua_i) = v_p(u) + v_p(a_i)$.

b), c) exercise. $\square$

Observation. $\varphi: R \rightarrow S$ a ring homomorphism. Then $\exists! \varphi_x: R[x] \rightarrow S[x]$ which extends φ and $\varphi_x(x) = x$.

In particular: for a Gaussian domain R and a prime factor p we have

$$\pi: R \twoheadrightarrow R/(p)$$

$$\pi_x: R[x] \twoheadrightarrow \left(R/(p)\right)[x]$$

Theorem 1.14 (Gauss's lemma). *Let R be a Gaussian domain. If $f, g \in R[x]$ are primitive polynomials, then $f \cdot g$ is primitive as well.*

Proof. We use: h primitive $\Leftrightarrow c_p(h) = 0, \forall p$.

Let p be a prime factor. We know that $c_p(f) = c_p(g) = 0$ and we want $c_p(fg) = 0$.

$R/(p)$ a domain $\xrightarrow{\text{exercise}} (R/(p))[x]$ a domain.

Clearly $c_p(h) = 0 \Leftrightarrow \pi_x(h) \neq 0$.

Hence $c_p(f) = c_p(g) = 0 \Rightarrow \pi_x(f) \neq 0, \pi_x(g) \neq 0$. Hence $\pi_x(fg) \stackrel{\text{hom}}{=} \pi_x(f) \cdot \pi_x(g) \stackrel{\text{domain}}{\neq} 0$. $\square$

Corollary 1.15. *For $f, g \in T[x] \setminus \{0\}$ and any prime factor $p \in R$ we have $c_p(fg) = c_p(f) + c_p(g)$.*

Proof. Let $u := \prod p^{-c_p(f)}$ and $v := \prod p^{-c_p(g)}$, where we multiply over pairwise non-associated prime factors p , and $f_1 := uf, g_1 := vg$.

For every p we have $c_p(f_1) = 0 = c_p(g_1) \Rightarrow f_1, g_1$ primitive. By Theorem 1.14, f_1g_1 is thus primitive $\Rightarrow c_p(f_1g_1) = 0$. But $f_1g_1 = uvfg$, so

$$0 = c_p(f_1g_1) = v_p(uv) + c_p(fg) = v_p(u) + v_p(v) + c_p(fg) = -c_p(f) - c_p(g) + c_p(fg). \quad \square$$

Proposition 1.16. *Let R be a Gaussian domain and T its field of fractions.*

Let $f, g \in R[x], \deg f \geq 1$ and f primitive.

a) $f \mid g$ in $T[x] \Rightarrow f \mid g$ in $R[x]$.

b) f irreducible in $R[x] \Leftrightarrow f$ irreducible in $T[x]$.

Proof. a) Let $g = qf, q \in T[x]$. f is primitive, so $c_p(g) = c_p(q)$ for all p . But $g \in R[x]$, hence $c_p(g) \geq 0$. Therefore $c_p(q) \geq 0$ and $q \in R[x]$. So we have proved that $f \mid g$ in $R[x]$.

b)

“ $\Leftarrow$ ” An easy exercise

“ $\Rightarrow$ ” Let f not be irreducible in $T[x]$, i.e. $f = f_1f_2$, where $f_1, f_2 \in T[x]$ are non-constant.

Similarly as in the proof of Corollary 1.15, for $u_1 = \prod p^{-c_p(f_1)}, u_2 = \prod p^{-c_p(f_2)}$ we have: $g_1 := u_1f_1$ and $g_2 := u_2f_2$ are primitive polynomials in $R[x]$. Moreover f primitive $\Rightarrow 0 = c_p(f) = c_p(f_1f_2) \stackrel{1.15}{=} c_p(f_1) + c_p(f_2)$.

Hence $u_1 \cdot u_2 = \prod p^{-(c_p(f_1)+c_p(f_2))} = \prod p^0 = 1$. Hence $f = f_1f_2 = (u_1u_2)^{-1}g_1g_2 = g_1g_2 \Rightarrow f$ is not irreducible in $R[x]$. $\square$

Proposition 1.17. *Let R be a Gaussian domain and T its field of fractions. The irreducible elements in $R[x]$ are exactly*

- the prime factors $p \in R$ and
- the primitive non-constant polynomials $f \in R[x]$ which are irreducible as elements of $T[x]$.

For every irreducible polynomial $g \in T[x]$ there is $u \in T$ such that ug is an irreducible element of the ring $R[x]$.

Proof. We want to describe the irreducible elements of $R[x]$; let us distinguish constant and non-constant polynomials in $R[x]$.

a) $f \in R$ (is a constant polynomial)

If $g \in R[x]$ satisfies $g \mid f$, then $g \in R$ must be constant as well. Hence $f \in R$ is irreducible in the ring $R[x] \Leftrightarrow f$ is irreducible in $R \Leftrightarrow f$ is a prime factor in R .

b) $f \in R[x], \deg f \geq 1$.

By Proposition 1.16b), the primitive polynomials $f \in R[x]$ which are irreducible in $T[x]$ are irreducible in $R[x]$.

Conversely, let a (non-constant) $f \in R[x]$ be irreducible in $R[x]$. Then $f = uf_1$, where $f_1 \in R[x]$ is primitive and $u = \prod p^{c_p(f)} \in R$.

But f irreducible $\Rightarrow u \parallel 1 \Rightarrow c_p(f) = 0, \forall p \Rightarrow f$ is primitive. Hence Proposition 1.16b) $\Rightarrow f$ is irreducible in $T[x]$.

2nd part of the proposition: Let $g \in T[x]$ be irreducible and define $v = \prod p^{-c_p(g)} \Rightarrow vg$ is a primitive element of $R[x]$ and $vg \parallel g$ in $T[x] \Rightarrow vg$ is irreducible in $T[x]$. Proposition 1.16b) $\Rightarrow vg$ is irreducible in $R[x]$. $\square$

Theorem 1.18. *If R is a Gaussian domain, then $R[x]$ is Gaussian as well.*

Proof. We use: R Gaussian $\Leftrightarrow$ 1. there are no infinite chains of proper divisors and 2. every irreducible element is a prime factor. (exercise)

1. Let $\dots f_i \mid f_{i-1} \mid \dots \mid f_2 \mid f_1, f_i \in R[x]$. Then $\deg f_1 \geq \deg f_2 \geq \dots \geq 0$, and hence $\exists k : \deg f_k = \deg f_{k+1} = \dots$.

Let a_i be the leading coefficient of $f_i \Rightarrow \dots \mid a_i \mid a_{i-1} \dots \mid a_2 \mid a_1$. This is a sequence of divisors in the Gaussian $R \Rightarrow \exists l : a_l \parallel a_{l+1} \parallel \dots$.

Hence for $i, j \geq \max\{k, l\}$ we have $\deg f_i = \deg f_j$ and $a_i \parallel a_j \Rightarrow f_i \parallel f_j$.

2. We want to prove that if $f \mid gh$ (in $R[x]$), then $f \mid g$ or $f \mid h$ (in $R[x]$). Let us have an irreducible element f in $R[x]$ and use Proposition 1.17, according to which we have two possibilities:

a) $f = p \in R$. Then $1 \leq c_p(gh) = c_p(g) + c_p(h)$, and hence $c_p(g) \geq 1$ or $c_p(h) \geq 1$. This implies that $p \mid g$ or $p \mid h$.

b) $\deg f \geq 1$ and f is primitive, irreducible in $T[x]$. $T[x]$ is Euclidean, hence Gaussian, and hence f is a prime factor in $T[x]$. At the same time $f \mid gh$ in $T[x]$.

WLOG let $f \mid g$ in $T[x]$. Proposition 1.16a) then implies $f \mid g$ in $R[x]$. $\square$

1.7 Chinese remainder theorem

We have already defined 3 operations on ideals, $I + J, IJ, I \cap J$, and we have: $I(J + K) = IJ + IK$ and $IJ \subset I \cap J$. (Exercise)

Definition. Ideals I, J in a ring R are comaximal if $I + J = R$.

Motivation:

1. If M is maximal, then $M + (a) = R$ for all $a \notin M$. Hence M, J are comaximal $\forall J \not\subset M$.

2. $R = \mathbb{Z}, I = (m), J = (n)$. Then $(m) + (n) = (\gcd(m, n))$. Hence $(m), (n)$ are comaximal if and only if m, n are coprime. So this is a variant of coprimality and a weakening of maximality (which corresponds to primes, which are coprime to everything they do not divide).

Lemma 1.19. I, J comaximal $\Rightarrow I \cap J = IJ$.

Proof. $I \cap J \stackrel{\text{comaximal}}{=} (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subset IJ + IJ = IJ$; the inclusion $IJ \subset I \cap J$ always holds. $\square$

Definition. Ideals $I_1, \dots, I_n < R$ are pairwise comaximal if I_j, I_k are comaximal for all $1 \leq j < k \leq n$.

Proposition 1.20. *Let $I_1, \dots, I_n$ be pairwise comaximal ideals in a ring R and $n \geq 2$. Then $I_1 \cap \dots \cap I_n = I_1 \cdots I_n$ and the pair $I_1 \cap \dots \cap I_{n-1}, I_n$ is comaximal.*

Proof. $I_1 \cdots I_{n-1}$ and I_n are comaximal:

Consider

$$\begin{aligned} R &= (I_1 + I_n)(I_2 + I_n) \cdots (I_{n-1} + I_n) \\ &= I_1 I_2 \cdots I_{n-1} + \text{further terms, which all contain } I_n \\ &\subset I_1 I_2 \cdots I_{n-1} + I_n \subset R. \end{aligned}$$

hence $I_1 \cdots I_{n-1} + I_n = R$. (Since $I_1 \cdots I_{n-1} \subset I_1 \cap \cdots \cap I_{n-1}$, the pair $I_1 \cap \cdots \cap I_{n-1}, I_n$ is comaximal as well.)

$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ we prove by induction. For $n = 2$ this is Lemma 1.19.

Let $n > 2$. Induction hypothesis: $I_1 \cap \cdots \cap I_{n-1} = I_1 \cdots I_{n-1}$.

From the 1st part of the proof: $I_1 \cdots I_{n-1}, I_n$ are comaximal. Then

$$(I_1 \cdots I_{n-1}) \cdot I_n \stackrel{1.19}{=} (I_1 \cdots I_{n-1}) \cap I_n \stackrel{\text{induction hypothesis}}{=} (I_1 \cap \cdots \cap I_{n-1}) \cap I_n. \quad \square$$

Proposition 1.21. *Let $I_1, \dots, I_n$ be ideals in a ring R . Consider the homomorphism*

$$\begin{aligned} \varphi: R &\rightarrow R/I_1 \times \cdots \times R/I_n \\ r &\mapsto (r + I_1, \dots, r + I_n). \end{aligned}$$

Then

- a) $\text{Ker } \varphi = I_1 \cap \cdots \cap I_n$,
- b) φ is surjective $\Leftrightarrow I_1, \dots, I_n$ are pairwise comaximal.

Proof. a) is clear.

b) “ $\Rightarrow$ ” Let φ be onto and $i \neq j$. We have

$$\begin{aligned} R &\xrightarrow{\varphi} R/I_1 \times \cdots \times R/I_n \twoheadrightarrow R/I_i \times R/I_j \twoheadrightarrow (R/I_i)/(I_i + I_j/I_i) \times (R/I_j)/(I_i + I_j/I_j) \\ &\stackrel{1.3}{\cong} R/I_i + I_j \times R/I_i + I_j. \end{aligned}$$

So this composition is surjective; however, it is the map $r \mapsto (r + I_i + I_j, r + I_i + I_j)$, i.e. in both components of the image we have the same value. Such a map is surjective only if $R/I_i + I_j$ has only 1 element.

Hence $I_i + I_j = R$ and I_i, I_j are comaximal.

“ $\Leftarrow$ ” Assume that $I_1, \dots, I_n$ are pairwise comaximal. By induction:

$n = 2$: We need that every $(r_1 + I_1, r_2 + I_2)$ lies in $\text{Im } \varphi$, i.e. that there is $r \in R$ such that $r \equiv r_i \pmod{I_i}$ for $i = 1, 2$.

Comaximality implies that $\exists a_1 \in I_1, a_2 \in I_2$ such that $1 = a_1 + a_2$. Now choose $r := r_1 a_2 + r_2 a_1$. Then $r - r_1 = (r_1 a_2 + r_2 a_1) - r_1(a_1 + a_2) = a_1(r_2 - r_1) \in I_1$. Similarly we get $r - r_2 \in I_2$.

Let $n \geq 3$. Consider $I := I_1 \cdots I_{n-1} \stackrel{1.20}{=} I_1 \cap \cdots \cap I_{n-1}$. Proposition 1.20 also implies that I, I_n are comaximal.

The induction hypothesis for 2 ideals: we have a surjection

$$\begin{aligned} \psi_1: R &\twoheadrightarrow R/I \times R/I_n, \\ r &\mapsto (r + I, r + I_n). \end{aligned}$$

For $n - 1$ we further have

$$\begin{aligned} \psi_2: R &\twoheadrightarrow R/I_1 \times \cdots \times R/I_{n-1}, \\ r &\mapsto (r + I_1, \dots, r + I_{n-1}). \end{aligned}$$

with $\text{Ker } \psi_2 = I_1 \cap \cdots \cap I_{n-1} = I$.

The 1st isomorphism theorem for ψ_2 then gives

$$\begin{aligned} \psi: R/I &\simeq R/I_1 \times \cdots \times R/I_{n-1}, \\ r + I &\mapsto (r + I_1, \dots, r + I_{n-1}). \end{aligned}$$

Finally, by composition we have

$$\varphi = (\psi \times \text{id}) \circ \psi_1: R \xrightarrow{\psi_1} R/I \times R/I_n \xrightarrow{\psi \times \text{id}} (R/I_1 \times \cdots \times R/I_{n-1}) \times R/I_n.$$

□

Corollary 1.22 (Chinese remainder theorem). *Let $I_1, \dots, I_n$ be pairwise comaximal ideals in R such that $I_1 \cap \cdots \cap I_n = \{0\}$. Then $\forall r_1, \dots, r_n \in R \exists! r \in R$ such that $r \equiv r_i \pmod{I_i}$ for all i .*

Remark. Let $n_1, \dots, n_k \in \mathbb{Z}$ be pairwise coprime and let $R = \mathbb{Z}/(n_1 \cdots n_k)$. Then

$$\mathbb{Z}/(n_1 \cdots n_k) \simeq \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k,$$

which gives the usual Chinese remainder theorem for integers.

1.8 Zorn's lemma

Let $\mathcal{A}$ be a set partially ordered by a relation $\leq$, i.e. it is

- reflexive: $x \leq x$,
- (weakly) antisymmetric: $x \leq y$ and $y \leq x \Rightarrow x = y$,
- transitive: $x \leq y \wedge y \leq z \Rightarrow x \leq z$

for all $x, y, z \in \mathcal{A}$.

A chain $\mathcal{B}$ in $\mathcal{A}$ is a subset which is linearly ordered, i.e. satisfies $\forall x, y \in \mathcal{B} : x \leq y$ or $y \leq x$.

An upper bound of a subset $\mathcal{C} \subset \mathcal{A}$ is an element $a \in \mathcal{A}$ such that $a \geq c$ for all $c \in \mathcal{C}$.

An element $a \in \mathcal{A}$ is maximal if $a \leq b$ implies $a = b$ for all $b \in \mathcal{A}$.

Axiom 1.23 (Zorn's lemma). *Let $\mathcal{A}$ be a non-empty set partially ordered by a relation $\leq$ such that every chain $\mathcal{B}$ in $\mathcal{A}$ has an upper bound. Then $\forall a \in \mathcal{A} \exists b \in \mathcal{A}$ such that b is maximal in $\mathcal{A}$ and $a \leq b$.*

This lemma is equivalent to the axiom of choice, which is one of the key axioms of set theory, although historically it was rather problematic (a number of mathematicians did not consider its validity to be self-evident). We, however, are interested in rings and not in set theory, so we will work with Zorn's lemma routinely (as is, after all, common today).

Example. Every vector space V has a basis.

$\mathcal{A} := \{\text{linearly independent subsets of } V\}$, $\leq$ is the ordering by inclusion, i.e. for $X, Y \in \mathcal{A}$ we define $X \leq Y$ if $X \subset Y$.

Now we have to verify the hypothesis of Zorn's lemma.

Let $\mathcal{B} \subset \mathcal{A}$ be a chain. We want an upper bound for it:

Choose $b \subset V$ as $b = \bigcup$ of the chain $\mathcal{B}$, i.e. $b = \{v \in V \mid \exists a \in \mathcal{B}, v \in a\}$. We need:

1. $b \in \mathcal{A}$. (I.e. b is linearly independent.)
2. $\forall a \in \mathcal{B} : a \leq b$.

Both are not hard to verify.

Hence by Zorn's lemma there is a maximal element $a \in \mathcal{A}$, i.e. a linearly independent set to which nothing can be added so that the result is still linearly independent.

For a contradiction, let a not be a basis, so $\exists v \in V \setminus \text{Span}(a)$. But then $a \cup \{v\}$ would be a larger linearly independent set, which would contradict the maximality of a . □

Now we show several useful applications of Zorn's lemma in ring theory.

Lemma 1.24. *Let A be a non-empty subset of a ring R and $I < R$. If $I \cap A = \emptyset$, then there is an ideal $J < R$ such that*

- $J \supset I$,
- $J \cap A = \emptyset$,
- $J' \cap A \neq \emptyset$ for every ideal $J' < R$ such that $J' \supsetneq J$.

Proof. Choose the set $\mathcal{A} = \{J < R \mid J \supset I, J \cap A = \emptyset\}$ ordered by inclusion $\subset$.

$\mathcal{A} \neq \emptyset$, because $I \in \mathcal{A}$.

Further, for a non-empty chain $\mathcal{B} \subset \mathcal{A}$ its upper bound is $\bigcup_{J \in \mathcal{B}} J \in \mathcal{A}$ (and the empty chain has the upper bound I).

The hypotheses are satisfied, so by Zorn's lemma 1.23 the set $\mathcal{A}$ has a maximal element J . It is easy to verify that it has all the required properties. $\square$

Corollary 1.25. *Let $I < R$ be a proper ideal. Then there is a maximal ideal M in R which contains I .*

Proof. In Lemma 1.24 choose $A = \{1\}$. $\square$

Warning! This corollary need not hold if R is a ring without 1! There even exist rings (without 1) which contain no maximal ideals.

Exercise: Think about which ideal J we get from the proof of Lemma 1.24 if we choose $A = \emptyset$.

Definition. A *multiplicative set* S in a ring R is a non-empty subset of R such that

- $0 \notin S$ and
- S is closed under multiplication, i.e. $a, b \in S \Rightarrow a \cdot b \in S$.

Proposition 1.26. *Let $S \subset R$ be a multiplicative set and $I < R$ an ideal such that $I \cap S = \emptyset$. Then there is a prime ideal $P \supset I$ such that $P \cap S = \emptyset$.*

Proof. In Lemma 1.24 choose $A = S$. It is then necessary to verify that the ideal J , which exists by this lemma, is a prime ideal: exercise. $\square$

Corollary 1.27. *For every multiplicative set S there is a prime ideal P such that $P \cap S = \emptyset$.*

Proof. Choose $I = \{0\}$ in Proposition 1.26. $\square$

2. Galois theory

2.1 Review

Let us recall some basic notions from the theory of (commutative) fields. Below, T, U, V are always fields such that $U \supset T$.

$U \supset T$ implies that U is a vector space over T . The degree of the field extension $d = [U : T]$ = the dimension of U as a vector space over T . Hence, if $d < \infty$, there is a basis $\alpha_1, \alpha_2, \dots, \alpha_d \in U$, i.e. $\forall \alpha \in U \exists! t_i \in T$ such that $\alpha = \sum t_i \alpha_i$.

If $V \supset U \supset T$, then $[V : T] = [V : U] \cdot [U : T]$.

$\alpha \in U$ is algebraic over T if it is a root of some $0 \neq f(x) \in T[x]$. If f has the minimal degree, it is the minimal polynomial of α .

For $\alpha \in U$ we define $T[\alpha]$ as the smallest subring of U which contains T and α , and $T(\alpha)$ as the smallest subfield of U which contains T and α .

If α is algebraic (over T), then $T[\alpha] = T(\alpha)$. We have $d = [T(\alpha) : T] = \deg$ of the minimal polynomial of α . As a basis of $T(\alpha)$ we can choose $1, \alpha, \dots, \alpha^{d-1}$.

If α is not algebraic (over T), then $T[\alpha] \simeq T[x]$ and $T(\alpha) \simeq T(x)$ (which is the ring of polynomials, resp. the field of rational functions).

Hence α is algebraic over $T \Leftrightarrow [T(\alpha) : T] < \infty$.

An extension $U \supset T$ is algebraic if every element $\alpha \in U$ is algebraic over T .

If an element α is algebraic, then $T(\alpha) \supset T$ is an algebraic extension.

$U \supset T$ an extension of finite degree $\Rightarrow U \supset T$ an algebraic extension.

T has characteristic p (which is necessarily a prime) if $1 + \dots + 1 = 0$ (and p is the smallest such number). If no such p exists, the characteristic is 0.

2.2 Introduction

Let $U \supset T, V \supset T$ be fields. A homomorphism $\varphi: U \rightarrow V$ is a T -homomorphism if $\varphi(t) = t$ for all $t \in T$.

Lemma 2.1. *Let $U \supset T, V \supset T$ be fields. Every T -homomorphism $\varphi: U \rightarrow V$ is injective.*

Proof. Consider the kernel $\text{Ker } \varphi$. It is an ideal in U , but a field contains only the ideals $\{0\}$ and U . Let $0 \neq t \in T$ be some element of the field T (here we use the fact that we do not consider a one-element set to be a field). Then $\varphi(t) = t$, because it is a T -homomorphism, and hence $t \notin \text{Ker } \varphi$, i.e. $\text{Ker } \varphi \neq U$.

Then $\text{Ker } \varphi = \{0\}$ and φ is injective, as we wanted. □

$\text{Gal}(U/T) = \{\varphi: U \rightarrow U \mid \varphi \text{ is a } T\text{-automorphism}\}$ is the Galois group of the extension $U \supset T$.

It is a group, because automorphisms can be composed and inverted; the identity id is the 1 of the group.

For example $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\text{id}, \varphi\}$, where $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, $\varphi(a + bi) = a - bi$.

Example. Let $D \in \mathbb{Z}$ be such that D is not a square. Consider the extension $\mathbb{Q}(\sqrt{D}) \supset \mathbb{Q}$. The minimal polynomial of $\sqrt{D}$ is $x^2 - D$.

Let $\varphi \in \text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$. Then

$$0 = \varphi(0) = \varphi((\sqrt{D})^2 - D) = \varphi(\sqrt{D})^2 - \varphi(D) = \varphi(\sqrt{D})^2 - D,$$

and hence $\varphi(\sqrt{D}) = \pm\sqrt{D}$.

Conversely, the value $\psi(\sqrt{D})$ uniquely determines $\psi \in \text{Gal}$: for $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ we have $\psi(a + b\sqrt{D}) = a + b\psi(\sqrt{D})$.

Hence $\text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) = \{\text{id}, \varphi\}$, where $\varphi(\sqrt{D}) = -\sqrt{D}$.

Especially if $U \supset T$ is an extension of finite degree, $\text{Gal}(U/T)$ gives a lot of information about the structure of this extension (and about the element α such that $U = T(\alpha)$). In Algebra you have seen, for example, its applications to ruler-and-compass constructions and to the unsolvability of the equation of degree 5.

2.3 Integral elements

Definition. Let R be a subring of S . An element $v \in S$ is *integral* over R if it is a root of some *monic* polynomial in $R[x]$, i.e. $\exists f \in R[x]$, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $f(v) = 0$.

Remark. If R, S are fields, then $v \in S$ is algebraic over $R \Leftrightarrow v \in S$ is integral over R .

Remark. Let $S = \mathbb{Q}$, $R = \mathbb{Z}$. Then $v \in \mathbb{Q}$ is integral over $\mathbb{Z} \Leftrightarrow v \in \mathbb{Z}$.

Proposition 2.2. Let R be a subring of a domain S and $v \in S$. The following statements are equivalent:

- 1) v is integral over R .
- 2) $R[v]$ is a finitely generated R -module.
- 3) There is a ring R' , $R[v] \subset R' \subset S$, such that R' is a finitely generated R -module.

Proof.

2) $\Rightarrow$ 3): We choose $R' = R[v]$.

1) $\Rightarrow$ 2): We know that $v^n + a_{n-1}v^{n-1} + \cdots + a_0 = 0$ for some $a_i \in R$.

We prove that $R[v] = R \cdot 1 + R \cdot v + \cdots + R \cdot v^{n-1} =: \heartsuit$.

“ $\supset$ ” Ok

“ $\subset$ ” $R[v] = \{\sum r_j v^j\}$. So it suffices to prove that $v^j \in \heartsuit$ for every j .

For $j = 0$ we have $v^0 = 1$. From the definition, for $0 \leq j \leq n-1$ we see that v^j is already in $\heartsuit$. What about v^n ?

$$v^n = -\underbrace{a_{n-1}v^{n-1}}_{\in R \cdot v^{n-1}} - \cdots - \underbrace{a_0}_{\in R \cdot 1} \in \heartsuit.$$

Let us continue by induction for $j \geq n+1$. We multiply the last equality by v^{j-n} and we have

$$v^j = -\underbrace{a_{n-1}v^{j-1}}_{\in \heartsuit} - \cdots - \underbrace{a_0 v^{j-n}}_{\in \heartsuit} \in \heartsuit.$$

3) $\Rightarrow$ 1) Let $R' = \sum_{j=1}^n R w_j$. Then for every i we have

$$v \cdot w_i = \sum_{j=1}^n a_{ij} w_j$$

for some $a_{ij} \in R$.

Let us look at these equations for $i = 1, \dots, n$ as at a system of homogeneous linear equations in the unknowns $w_1, \dots, w_n$ and with coefficients from the field of fractions of the domain S .

Not all w_j are 0 (since $1 \in R'$) $\Rightarrow$ the system has a nontrivial solution $\Rightarrow$ determinant = 0.

The matrix of the system is

$$\begin{pmatrix} v - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & v - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & v - a_{nn} \end{pmatrix},$$

so its determinant is a polynomial in the variable v with coefficients in R and with leading term $1 \cdot v^n$ – more precisely, the determinant equals the value $f(v)$ for some monic polynomial $f \in R[x]$. This f is thus the desired monic polynomial for v . $\square$

Remark. Proposition 2.2 holds even if S is not a domain (with more or less the same proof).

Corollary 2.3. *The set of elements of a domain S which are integral over $R \subset S$ forms a subring in S (containing R).*

Proof. Let $a, b \in S$ be integral over R . Then $R[a]$ is a finitely generated R -module.

b is also integral over $R[a]$, and hence $R[a][b] = R[a, b]$ is a finitely generated $R[a]$ -module.

Exercise $\Rightarrow R[a, b]$ is a finitely generated R -module.

For $v = a \pm b, a \cdot b$ we have $R[v] \subset R[a, b]$, and hence v is integral by Proposition 2.2. $\square$

2.4 Root fields and splitting fields

Definition. Let $S \supset T$ be a field extension, $f(x) \in T[x]$. S is a root field of the polynomial f if f has a root $\alpha \in S$ and $S = T(\alpha)$.

S is a splitting field of the polynomial f if f splits in $S[x]$ into linear factors $f(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n)$, where $c, \alpha_i \in S$ and $S = T(\alpha_1, \dots, \alpha_n)$.

Proposition 2.4. *Let T be a field and $f \in T[x]$ a polynomial of degree ≥ 1 . Then*

(a) *there is a root field for f over T and*

(b) *there is a splitting field for f over T .*

Proof. a) Let $g \mid f$ be irreducible and consider the ideal $(g) = gT[x] < T[x]$.

g is irreducible $\Rightarrow (g)$ is maximal $\xrightarrow{1.7} S := T[x]/(g)$ is a field. We prove that it is the desired root field.

We have the projection

$$\begin{aligned} \pi: T[x] &\twoheadrightarrow S \\ h &\mapsto h + (g) \end{aligned}$$

Further, consider the restriction of the homomorphism π to $T \subset T[x]$, i.e. $\pi \upharpoonright T : T \rightarrow S$. This restriction is injective, because if $0 + (g) = (\pi \upharpoonright T)(t) = \pi(t) = t + (g)$, then $t \in (g)$, which is possible only for $t = 0$, since the degree of all nonzero polynomials in (g) is $\geq \deg g \geq 1$.

We may thus identify T with its image $\text{Im}(\pi \upharpoonright T) \subset S$ and assume that $T \subset S$. Moreover, note that then π fixes the elements of T , i.e. it is a T -homomorphism. Since $\pi : T[x] \rightarrow S$ is a surjective T -homomorphism, we have $S = T[\pi(x)]$.

Consider now the polynomial ring $S[X]$ in the variable X over S . We have $g(X) \in T[X] \subset S[X]$. We have $\pi(x) \in S$, and hence we can substitute this value into $g(X)$:

$$g(\pi(x)) = \sum_i a_i \pi(x)^i = \pi \left(\sum_i a_i x^i \right) = \pi(g) = 0.$$

Hence the polynomial $g \mid f$ has the root $\pi(x) \in S$. We have already seen that $S = T[\pi(x)]$.

b) By induction on the degree $\deg f$.

For $\deg f = 1$ the splitting field is $S = T$.

For $\deg f > 1$ let $T(\alpha)$ be a root field of f over T . Then $f(x) = g(x) \cdot (x - \alpha)$. The polynomial $g(x)$ over $T(\alpha)$ has degree $\deg f - 1$, hence there is a splitting field for it over $T(\alpha)$

$$S = T(\alpha)(\alpha_1, \dots, \alpha_m) = T(\alpha, \alpha_1, \dots, \alpha_m).$$

This is the desired splitting field for f over T . □

Now we prove the uniqueness of root fields and splitting fields up to T -isomorphism.

Lemma 2.5. *Let T be a field, $f \in T[x]$ an irreducible (non-constant) polynomial. If S_1, S_2 are root fields for f over T , then there is a T -isomorphism $\varphi : S_1 \rightarrow S_2$.*

Example. This lemma does not hold in general if f is reducible. Choose for example $f(x) = x(x^2 + 1)$ and $T = \mathbb{Q}$. The polynomial f has the roots $0, \pm i$.

Hence $S_1 = \mathbb{Q}$ and $S_2 = \mathbb{Q}(i)$ are its root fields, but $\mathbb{Q} \not\cong \mathbb{Q}(i)$.

Proof. Let $S_1 = T(\alpha), S_2 = T(\beta)$.

We know that $T(\alpha) = T[\alpha] = \{g(\alpha) \mid g \in T[x]\}$ and similarly for $T(\beta)$.

Consider

$$\begin{aligned} \varphi : T(\alpha) &\rightarrow T(\beta) \\ g(\alpha) &\mapsto g(\beta) \end{aligned}$$

Is it well defined? Note that f is (up to a nonzero constant) the minimal polynomial of both α and β , hence $g(\alpha) = h(\alpha) \Leftrightarrow (g-h)(\alpha) = 0 \Leftrightarrow_{f \text{ min. pol. of } \alpha} f \mid g-h \Leftrightarrow_{f \text{ min. pol. of } \beta} (g-h)(\beta) = 0 \Leftrightarrow g(\beta) = h(\beta)$.

Hence φ is well defined and injective. *Onto* is clear from the definition.

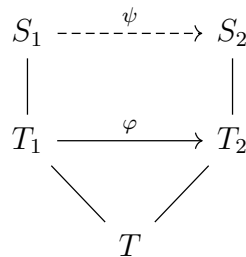
Clearly it is a T -homomorphism, so we have a T -isomorphism. □

Proposition 2.6. *Let us have field extensions $T_1, T_2 \supset T$ and a T -isomorphism $\varphi : T_1 \rightarrow T_2$.*

For $f(x) = \sum a_i x^i \in T_1[x]$ we define $\varphi(f)(x) := \sum \varphi(a_i) x^i \in T_2[x]$.

Let $\deg f \geq 1$ and $S_1 =$ a splitting field of f over T_1 , $S_2 =$ a splitting field of $\varphi(f)$ over T_2 .

Then there is a T -isomorphism $\psi : S_1 \rightarrow S_2$ such that $\psi \upharpoonright T_1 = \varphi$.



Choosing $T = T_1 = T_2$ and $\varphi = \text{id}$ in Proposition 2.6 we get:

Theorem 2.7. *Let T be a field and $f \in T[x]$ a non-constant polynomial. The splitting field of f over T is uniquely determined up to T -isomorphism.*

Proof of Proposition 2.6. By induction on $\deg f$:

$\deg f = 1$: We have $S_1 = T_1, S_2 = T_2, \psi = \varphi$.

$\deg f > 1$: Let $g \mid f$ be an irreducible polynomial in $T_1[x]$ and $\alpha \in S_1$ a root of g . Then $\varphi(g) \mid \varphi(f)$ (and $\varphi(g)$ is irreducible in $T_2[x]$); let $\beta \in S_2$ be a root of $\varphi(g)$. Similarly as in Lemma 2.5 we have a T -isomorphism

$$\begin{aligned} \sigma: T_1(\alpha) &\rightarrow T_2(\beta) \\ h(\alpha) &\mapsto \varphi(h)(\beta) \end{aligned}$$

(we use: g is the minimal polynomial of α over T_1 and $\varphi(g)$ is the minimal polynomial of β .)

Moreover $\sigma \upharpoonright T_1 = \varphi$.

Let $h \in T_1(\alpha)[x]$ be such that $f(x) = (x - \alpha)h(x)$; then $\sigma(f)(x) = (x - \beta)\sigma(h)(x)$, because by definition $\beta = \sigma(\alpha)$.

We see that S_1, S_2 are splitting fields for $h, \sigma(h)$ over $T_1(\alpha), T_2(\beta)$.

$\deg h < \deg f \Rightarrow$ by the induction hypothesis we have a T -isomorphism $\psi: S_1 \rightarrow S_2$ such that $\psi \upharpoonright T_1(\alpha) = \sigma$, and hence $\psi \upharpoonright T_1 = \sigma \upharpoonright T_1 = \varphi$.

$$\begin{array}{ccc} S_1 & \xrightarrow{\psi} & S_2 \\ | & & | \\ T_1(\alpha) & \xrightarrow{\sigma} & T_2(\beta) \\ | & & | \\ T_1 & \xrightarrow{\varphi} & T_2 \\ & \searrow & \swarrow \\ & T & \end{array}$$

□

2.5 Algebraic closure

Definition. A field T is algebraically closed if every non-constant polynomial from $T[x]$ has a root in T .

Equivalently: Every polynomial from $T[x]$ splits into linear factors.

Example. $\mathbb{C}$ is algebraically closed.

No finite field is algebraically closed (exercise).

Definition. Let T be a field. Its *algebraic closure* is an algebraically closed field $S \supset T$ which is an algebraic extension of T .

The algebraic closure of a field T is often denoted $\overline{T}$.

Example. $\pi, e \in \mathbb{C}$ are transcendental over $\mathbb{Q} \Rightarrow \mathbb{C}$ is not the algebraic closure of $\mathbb{Q}$.

$\mathbb{C} = \mathbb{R}(i)$ is the algebraic closure of $\mathbb{R}$.

We will gradually prove that the algebraic closure of every field exists and is unique (up to T -isomorphism).

We will not need the following proposition in the rest of the text, but it allows us, for example, to describe what $\overline{\mathbb{Q}}$ looks like. Indeed, from Algebra we know that $\mathbb{C}$ is algebraically closed, and hence the proposition implies that $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$.

Proposition 2.8. *Let us have fields $S \supset T$ and let $U = \{\alpha \in S \mid \alpha \text{ is algebraic over } T\}$, which is a field $T \subset U \subset S$. If S is algebraically closed, then U is an algebraic closure of T .*

Proof. From Algebra we know that U is a field. Clearly $U \supset T$ is an algebraic extension. Is U algebraically closed?

Let $f \in U[x]$ be non-constant. S algebraically closed $\Rightarrow f$ has a root $\beta \in S$. We want $\beta \in U$.

Let $f(x) = \sum \alpha_i x^i, \alpha_i \in U$. Then $f \in T(\alpha_0, \dots, \alpha_n)[x]$, so β is algebraic over $T(\alpha_0, \dots, \alpha_n)$, i.e. $[T(\alpha_0, \dots, \alpha_n, \beta) : T(\alpha_0, \dots, \alpha_n)] < \infty$.

Every α_i is algebraic over $T \Rightarrow [T(\alpha_0, \dots, \alpha_n) : T] < \infty$. Hence $[T(\alpha_0, \dots, \alpha_n, \beta) : T] < \infty \Rightarrow \beta$ is algebraic over $T \Rightarrow \beta \in U$. $\square$

Example. The algebraic closure of $\mathbb{Q}$ exists and is countable (but $\mathbb{C}$ is uncountable).

Lemma 2.9. *For every field T there is an algebraic extension $S \supset T$ such that every non-constant polynomial from $T[x]$ has a root in S .*

Proof. It is proved similarly to the existence of a root field in Proposition 2.4, but we need to add the roots of all polynomials at once.

For every non-constant irreducible polynomial $f \in T[x]$ choose a variable x_f and let $X = \{x_f \mid f \in T[x] \text{ non-constant irreducible}\}$. Consider $T[X] :=$ polynomials in the variables X (each polynomial, however, contains only finitely many of them).

We want a factor ring where $x_f \mapsto$ a root of the polynomial f :

Let $I = (f(x_f) \mid f \in T[x] \text{ non-constant irreducible}) < T[X]$ be the ideal generated by all the $f(x_f)$.

Exercise: $1 \notin I$.

Proof. Suppose for a contradiction that $1 \in I$. This means that $1 = \sum f(x_f)g_f$ for some polynomials $g_f \in T[X]$. On the right-hand side we have a finite sum, so only finitely many variables x_h occur in it. Consider $H :=$ the product of all polynomials h such that the variable x_h occurs in the equality, and let U be a splitting field of the polynomial H .

In the field U every such polynomial h thus has a root α_h . Substituting $x_h \mapsto \alpha_h$ into the equality we get $1 = \sum f(\alpha_f)g_f(\dots) = \sum 0 \cdot g_f(\dots) = 0$, which is a contradiction. $\square$

By Zorn's lemma there is a maximal ideal $M < T[X]$ such that $I \subset M$ (Corollary 1.25). Then the factor ring $S := T[X]/M$ is a field and we have $T \hookrightarrow S$ (as in Proposition 2.4). Every non-constant irreducible polynomial $f \in T[x]$ has a root in S , namely $x_f + M$. Hence reducible polynomials have roots as well.

Moreover, S arises by adding all these algebraic elements $x_f + M$ to T (because we have a surjective T -homomorphism $T[X] \twoheadrightarrow S$), and therefore it is an algebraic extension. $\square$

Theorem 2.10. *For every field T its algebraic closure exists. Any two algebraic closures of a field T are T -isomorphic.*

Proof.

Existence: Let $T = S_0 \subset S_1 \subset \dots$ be a chain of fields, where S_{i+1} arises from S_i by applying Lemma 2.9. Let $S = \bigcup S_i$. Clearly: S is a field which is an algebraic extension of T , because every element $\alpha \in S$ lies in some S_i , which is an algebraic extension of T .

S is algebraically closed, because for every $f \in S[x]$ there is i such that $f \in S_i[x]$, and hence f has a root in $S_{i+1} \subset S$.

Hence S is an algebraic closure of T .

Uniqueness: Let S_1, S_2 be algebraic closures of the field T .

Observation: If $S_1 \subset S_2$, then $S_1 = S_2$.

Proof of the observation. Let $\alpha \in S_2 \Rightarrow \alpha$ is a root of some $f \in T[x]$.

S_1 algebraically closed $\Rightarrow f(x) = c \prod (x - \alpha_i)$, where $\alpha_i, c \in S_1 \Rightarrow \exists i : \alpha = \alpha_i \in S_1$.

Hence $S_1 = S_2$. □

In general, consider the set

$$\mathcal{M} := \{\varphi : U_1^\varphi \rightarrow U_2^\varphi \text{ } T\text{-isomorphism} \mid T \subset U_1^\varphi \subset S_1, T \subset U_2^\varphi = \varphi(U_1^\varphi) \subset S_2\}$$

(we use the notation U_1^φ, U_2^φ to emphasize that these fields belong to φ : formally correctly we should define $\mathcal{M}$ as the set of ordered triples $(\varphi, U_1^\varphi, U_2^\varphi)$).

We order the set $\mathcal{M}$ by defining

$$\varphi \leq \psi, \text{ if } U_1^\psi \supset U_1^\varphi, U_2^\psi \supset U_2^\varphi \text{ and } \psi \upharpoonright U_1^\varphi = \varphi.$$

Let us now verify the hypotheses of Zorn's lemma 1.23:

$\mathcal{M} \neq \emptyset$, because it contains $\text{id} : T \rightarrow T$.

"The upper bound of a chain" $\mathcal{B}$ is again an element of $\mathcal{M}$: exercise; take $U_i = \bigcup_{\varphi \in \mathcal{B}} U_i^\varphi$ and define the new $\psi : U_1 \rightarrow U_2$ elementwise.

By Zorn's lemma there is thus a maximal element $\varphi : U_1 \rightarrow U_2$ in $\mathcal{M}$.

I want: φ is a T -isomorphism $S_1 \rightarrow S_2$.

Let $U_1 \neq S_1 \Rightarrow U_1 \subsetneq S_1 \Rightarrow U_1$ is not algebraically closed (by the observation above) $\Rightarrow \exists f(x) = \sum a_i x^i \in U_1[x]$ which has no root in U_1 . Let $V_1 \subset S_1$ be a splitting field for f over U_1 and $V_2 \subset S_2$ a splitting field for $\varphi(f) := \sum \varphi(a_i) x^i$ over U_2 .

By Proposition 2.6 there is a T -isomorphism $\psi : V_1 \rightarrow V_2$ such that $\psi \upharpoonright U_1 = \varphi$, which however contradicts the maximality of φ , and hence $U_1 = S_1$.

$\varphi : U_1 \rightarrow U_2$ is a T -isomorphism and $U_1 = S_1$ is an algebraic closure. Hence $U_2 \subset S_2$ are two algebraic closures. The observation $\Rightarrow U_2 = S_2$. □

Similarly one proves

Corollary 2.11.

a) Let us have fields $T \subset U \subset K, T \subset V \subset K$, where $K = \overline{T}$ is the algebraic closure of T . Then for every T -homomorphism $\varphi : U \rightarrow V$ there is a T -automorphism $\psi : K \rightarrow K$ which extends φ , i.e. $\psi \upharpoonright U = \varphi$.

b) Let $T \subset U \subset W \subset K$, where $K = \overline{T}$ is the algebraic closure of T . For every T -homomorphism $\varphi : U \rightarrow K$ there is a T -homomorphism $\sigma : W \rightarrow K$ such that $\sigma \upharpoonright U = \varphi$

Proof. We only sketch the proof.

a) $\Rightarrow$ b) is easy: it suffices to take $V = K$ and $\sigma = \psi \upharpoonright W$.

For a) it suffices to prove it for a T -isomorphism φ , because

Exercise. Let $\varphi : U \rightarrow V$ be a T -homomorphism. Then φ is injective, and hence it gives a T -isomorphism $U \rightarrow \text{Im}(\varphi)$.

For the proof it is now necessary to extend $\varphi : U \rightarrow V$ to a maximal T -isomorphism using Zorn's lemma, similarly as in the previous proof. □

This result is also often useful:

Exercise. Let $T \subset U$ be an algebraic extension and $U \subset K$. Then K is an algebraic closure of $T \Leftrightarrow K$ is an algebraic closure of U .

2.6 The Galois group

Recall that for a field extension $U \supset T$ the Galois group is $\text{Gal}(U/T) = \{T\text{-automorphisms } \varphi : U \rightarrow U\}$.

Proposition 2.12. *Let us have fields $U, V \supset T$ and a nonzero polynomial $f \in T[x]$.*

- a) *Every T -homomorphism $\varphi : U \rightarrow V$ maps each root of f in U to a root of f in V .*
b) *Let M be the set of all roots of f in the field U . If $\varphi : U \rightarrow U$ is a T -homomorphism, then $\varphi \upharpoonright M$ is a permutation of the set M .*

In particular, part b) holds for every $\varphi \in \text{Gal}(U/T)$.

Proof. a) Let $f(x) = \sum a_i x^i \in T[x]$ and let $u \in U$ be its root. Then $\varphi(u)$ is also a root of f , because

$$f(\varphi(u)) = \sum a_i (\varphi(u))^i \stackrel{T\text{-hom}}{=} \varphi\left(\sum a_i u^i\right) = \varphi(f(u)) = \varphi(0) = 0.$$

b) By part a) for $V = U$ we have $\varphi \upharpoonright M : M \rightarrow M$.

Thanks to Lemma 2.1, φ is injective $\Rightarrow \varphi \upharpoonright M$ is injective.

M finite $\Rightarrow \varphi \upharpoonright M$ is a permutation. □

Proposition 2.13. *Let U be a splitting field of a polynomial $f \in T[x]$ and $\deg f = n \geq 1$.*

- a) *The Galois group embeds into the symmetric group S_n , i.e. we have*

$$\begin{aligned} \text{Gal}(U/T) &\hookrightarrow S_n \\ \varphi &\mapsto \varphi \upharpoonright M \end{aligned}$$

b) *If f is irreducible over T , then for any two roots $\alpha, \beta \in U$ there is $\varphi \in \text{Gal}(U/T)$ such that $\varphi(\alpha) = \beta$.*

Proof. a) Let $M = \{\alpha_1, \dots, \alpha_k\}$ be the set of roots of f . By Proposition 2.12b), $\varphi \upharpoonright M$ is a permutation of the k -element set M for every $\varphi \in \text{Gal}(U/T)$, hence it gives an element of S_k . We extend this permutation to a permutation from S_n by defining it as the identity for $i = k + 1, \dots, n$. So we get the map

$$\begin{aligned} \text{Gal}(U/T) &\rightarrow S_n \\ \varphi &\mapsto \varphi \upharpoonright M \end{aligned}$$

It is easy to check that it is a homomorphism (exercise).

By the definition of a splitting field we have $U = T(\alpha_1, \dots, \alpha_k)$, and hence φ is uniquely determined by its values $\varphi(\alpha_1), \dots, \varphi(\alpha_k)$, i.e. exactly by the restriction $\varphi \upharpoonright M$. The map $\varphi \mapsto \varphi \upharpoonright M$ is therefore injective.

b) f irreducible $\Rightarrow$ the root fields $T(\alpha), T(\beta)$ are T -isomorphic by Lemma 2.5. So we have a T -isomorphism $\varphi : T(\alpha) \rightarrow T(\beta)$ such that $\varphi(\alpha) = \beta$. By Proposition 2.6 we can then extend φ to a T -isomorphism $\psi : U \rightarrow U$ (we choose $T_1 = T(\alpha), T_2 = T(\beta), S_1 = S_2 = U$).

Hence $\psi \in \text{Gal}(U/T)$ and $\psi(\alpha) = \beta$. □

2.7 Separable extensions

Let $f \in \mathbb{Q}[x]$ and let $T = \mathbb{Q}(\alpha)$ be its root field. Consider a $\mathbb{Q}$ -homomorphism into the algebraic closure $\varphi : \mathbb{Q}(\alpha) \rightarrow \overline{\mathbb{Q}}$ (see Proposition 2.8 for a description of $\overline{\mathbb{Q}}$).

φ is uniquely determined by the value $\varphi(\alpha)$, which must be a root of f in $\overline{\mathbb{Q}}$ by Proposition 2.12a). The polynomial f has at most $\deg f$ roots, and hence there are at most $\deg f$ distinct $\mathbb{Q}$ -homomorphisms $\varphi: \mathbb{Q}(\alpha) \rightarrow \overline{\mathbb{Q}}$.

If f is irreducible over $\mathbb{Q}$, then the number of φ equals $\deg f$ (because an irreducible polynomial has no multiple roots in $\mathbb{C} \supset \overline{\mathbb{Q}}$ – see for example Proposition 2.18 below).

In general, the number of φ can be $< \deg f$ even for an irreducible polynomial f , if T has positive characteristic.

For example, choose $T = \mathbb{F}_p(y)$ and $f(x) = x^p - y \in T[x]$. This polynomial is irreducible over T by Eisenstein's criterion, but $f(x) = (x - \sqrt[p]{y})^p$ over its root field $T(\sqrt[p]{y})$ (and hence also over the algebraic closure). Hence the only $\varphi: T(\sqrt[p]{y}) \rightarrow \overline{T}$ is the identity and the number of $\varphi = 1$.

Definition. Let $T \subset U \subset \overline{T}$ be fields, where $\overline{T}$ = the algebraic closure of T . The cardinality of the set $\{\varphi: U \rightarrow \overline{T} \mid T\text{-homomorphism}\}$ is called the *separability degree* of the extension $U \supset T$ and is denoted $[U : T]_s$.

Proposition 2.14. *Let us have algebraic extensions $T \subset U \subset V$. Then*

$$[V : T]_s = [V : U]_s \cdot [U : T]_s.$$

Proof. It suffices to prove the following observation:

Observation: Let $\overline{T}$ be an algebraic closure of T and define

$$\Phi = \{\varphi: U \rightarrow \overline{T} \mid T\text{-homomorphism}\}, \Psi = \{\psi: V \rightarrow \overline{T} \mid U\text{-homomorphism}\}.$$

For $\varphi \in \Phi$ choose $\overline{\varphi}: \overline{T} \rightarrow \overline{T}$ some T -automorphism extending φ (by Corollary 2.11a).

Then $\{\overline{\varphi} \circ \psi \mid \varphi \in \Phi, \psi \in \Psi\}$ is the set of all T -homomorphisms $V \rightarrow \overline{T}$.

Moreover, $\overline{\varphi}_1 \circ \psi_1 = \overline{\varphi}_2 \circ \psi_2$ implies $\varphi_1 = \varphi_2$ and $\psi_1 = \psi_2$.

Proof of the observation. Let $\rho: V \rightarrow \overline{T}$ be a T -homomorphism. Then we can choose $\varphi := \rho \upharpoonright U \in \Phi$ and $\psi := \overline{\varphi}^{-1} \circ \rho \in \Psi$ (exercise: why is ψ a U -homomorphism?) to get $\rho = \overline{\varphi} \circ \psi$.

If $\overline{\varphi}_1 \circ \psi_1 = \overline{\varphi}_2 \circ \psi_2$, then $\varphi_1(u) = \overline{\varphi}_1(u) = \overline{\varphi}_1 \circ \psi_1(u) = \overline{\varphi}_2 \circ \psi_2(u) = \varphi_2(u)$ for every $u \in U$. Hence $\varphi_1 = \varphi_2$, so $\overline{\varphi}_1 = \overline{\varphi}_2$, and finally $\psi_1 = \psi_2$ (because $\overline{\varphi}_1 = \overline{\varphi}_2$ is a bijection). $\square$

Lemma 2.15. *Let $U \supset T$ be a field extension of finite degree.*

a) *Then $[U : T]_s \leq [U : T]$.*

b) *If $\alpha \in U$ is an element such that the degree of the minimal polynomial m of α over T is n and the polynomial m has exactly k roots in the algebraic closure, then*

$$[U : T]_s \leq \frac{k}{n} [U : T].$$

Proof. a) If $U = T(\beta)$, then $[T(\beta) : T]_s \leq [T(\beta) : T]$ (because $\varphi(\beta)$ is a root of the minimal polynomial of β). In general we have $U = T(\beta_1, \dots, \beta_l)$ and we can use induction by means of Proposition 2.14.

b) We have $T \subset T(\alpha) \subset U$, and hence

$$[U : T] = [U : T(\alpha)] \cdot [T(\alpha) : T] = [U : T(\alpha)] \cdot n.$$

Then

$$[U : T]_s \stackrel{2.14}{=} [U : T(\alpha)]_s \cdot [T(\alpha) : T]_s = [U : T(\alpha)]_s \cdot k \stackrel{\text{part a)}}{\leq} [U : T(\alpha)] \cdot k = \frac{[U : T]}{n} \cdot k. \quad \square$$

Definition. Let T be a field. A polynomial $f \in T[x]$ is a *separable polynomial* if it has no multiple roots in the algebraic closure $\overline{T}$.

If $T \subset U$ and $\alpha \in U$, then α is a *separable element* if α is algebraic over T and its minimal polynomial is separable.

An extension $U \supset T$ is a *separable extension* if all elements $\alpha \in U$ are separable.

Proposition 2.16. *Let $U \supset T$ be a field extension of finite degree. The following statements are equivalent:*

1. $U = T(\alpha_1, \dots, \alpha_k)$ for separable α_i ,
2. $[U : T] = [U : T]_s$,
3. $U \supset T$ is a separable extension.

Proof.

3) $\Rightarrow$ 1) $U \supset T$ is an extension of finite degree, and hence $U = T(\alpha_1, \dots, \alpha_k)$ for some elements $\alpha_i \in U$. These elements are separable, because $U \supset T$ is a separable extension.

1) $\Rightarrow$ 2) If $k = 1$ and $U = T(\alpha)$, then $[U : T]_s = \#$ of roots (in the algebraic closure) of the minimal polynomial of $\alpha = \deg$ of the minimal polynomial $= [U : T]$.

For $k > 1$ we proceed by induction using Proposition 2.14 (note that α_k is separable also over $T(\alpha_1, \dots, \alpha_{k-1})$, because its minimal polynomial over this field divides its minimal polynomial over T).

2) $\Rightarrow$ 3) If there were $\alpha \in U$ which is not separable over T , then by Lemma 2.15b) we would have $[U : T]_s < [U : T]$, since $k < n$. $\square$

Exercise: An element is separable $\Leftrightarrow$ it is a root of some separable polynomial.

Exercise: Let us have a field extension $U \supset T$. All elements $\alpha \in U$ which are separable over T form a subfield of U , the so-called separable closure of T in U .

Proposition 2.17. *If U is a separable extension of a field T and V a separable extension of the field U , then V is a separable extension of the field T .*

Proof. We cannot use Proposition 2.16 right away, because we do not necessarily have extensions of finite degree. Therefore we carry out the proof elementwise (similarly as the analogous property was proved for algebraic extensions!).

Let $\alpha \in V$ and let $m(x) = \sum_{i=0}^n a_i x^i$ be the minimal polynomial of α over U . Let $U_1 = T(a_0, \dots, a_n)$ and $V_1 = U_1(\alpha)$. We see that $U_1 \supset T$ and $V_1 \supset U_1$ are of finite degree.

Condition 1) of Proposition 2.16 is satisfied for $U_1 \supset T$, so condition 2) $[U_1 : T]_s = [U_1 : T]$ holds. In the same way we have $[V_1 : U_1]_s = [V_1 : U_1]$.

Multiplying them we get $[V_1 : T]_s = [V_1 : T]$, and hence again by Proposition 2.16, $V_1 \supset T$ is a separable extension. Finally, therefore, $\alpha \in V_1$ is a separable element over T . $\square$

Irreducible inseparable polynomials are rather unusual, so let us prove quite strong necessary conditions for their existence.

Proposition 2.18. *Let T be a field and $f(x) = \sum a_i x^i$ a (non-constant) irreducible inseparable polynomial. Then*

- a) T has characteristic $p > 0$,
- b) $\exists i : a_i \neq b^p$ for all $b \in T$ and
- c) $\exists g \in T[x] : f(x) = g(x^p)$, i.e. $a_i = 0$ if $p \nmid i$.

For the proof we need to use the formal derivative of a polynomial.

Observation. For a polynomial $f(x) = \sum a_i x^i$ we define its formal derivative as $f'(x) = \sum i a_i x^{i-1}$. Among other things, it is useful for detecting multiple roots:

If $f(x) = (x - \alpha)^k \cdot g(x)$, then

$$f'(x) = [(x - \alpha)^k \cdot g(x)]' = k(x - \alpha)^{k-1}g(x) + (x - \alpha)^k g'(x) = (x - \alpha)^{k-1}(\text{something}).$$

Hence $(x - \alpha)^{k-1}$ is a common divisor of f and f' .

Proof of Proposition 2.18. a) Since f is inseparable, it has a multiple root $\alpha \in \overline{T}$ (of multiplicity $k \geq 2$). Hence the corresponding $(x - \alpha)^{k-1}$ is a common divisor of f and f' , and so $\gcd(f, f') \nmid 1$. At the same time $\gcd(f, f') \mid f$ and f is irreducible, hence $\gcd(f, f') \parallel f$.

We have $f \parallel \gcd(f, f') \mid f'$. But $\deg f' < \deg f$, and hence $f' = 0$, i.e. $i a_i = 0 \forall i$. However, some coefficient a_i with $i \geq 1$ is nonzero, and hence the characteristic of the field T is not 0, so it equals some prime p .

c) If $p \nmid i$, then $i a_i = 0$ implies $a_i = 0$, and hence $f(x) = g(x^p)$ for $g(x) = \sum a_{pi} x^i$.

b) By contradiction. If $a_i = b_i^p$ for every i , then

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots = b_0^p + b_p^p x^p + b_{2p}^p x^{2p} + \cdots = (b_0 + b_p x + b_{2p} x^2 + \cdots)^p,$$

which contradicts the irreducibility of f . □

Definition. A field T is perfect if it has characteristic 0, or it has characteristic p and the “Frobenius map” $x \mapsto x^p$ is an automorphism.

Hence over a perfect field there are no irreducible inseparable polynomials. For example, $\mathbb{F}_p$ is perfect, because $x = x^p$ (and similarly every finite field is perfect).

Every algebraically closed field is also perfect.

Corollary 2.19. *Every algebraic extension of a perfect field is separable.*

2.8 Simple extensions

Definition. An extension $U \supset T$ is simple if $U = T(\alpha)$ for some element $\alpha \in U$ which is algebraic over T .

Theorem 2.20. *Every separable field extension of finite degree is simple.*

Proof. Let $U \supset T$ be a finite separable extension. We distinguish two cases:

1. T is a finite field $\Rightarrow U$ is also finite $\Rightarrow U^\times = U \setminus \{0\}$ is a cyclic (multiplicative) group (from Algebra we know the statement that *every finite multiplicative subgroup of a field is cyclic*). If α is its generator, then $U = T(\alpha)$.

2. T is infinite. Let $\alpha \in U$ be such that $[T(\alpha) : T]$ is the largest possible (the maximum exists, because $[T(\alpha) : T] \leq [U : T] < \infty$). We want to prove that $T(\alpha) = U$. Suppose for a contradiction that this does not hold.

Let $\beta \in U \setminus T(\alpha)$ and $V = T(\alpha, \beta)$. It suffices to prove that $V = T(\gamma)$ for some γ , because then $[T(\gamma) : T] > [T(\alpha) : T]$.

$U \supset T$ is separable, so $V \supset T$ is a separable extension of finite degree. Consider all the T -homomorphisms $f_1, \dots, f_n : V \rightarrow \overline{T}$, where $\overline{T} = \overline{V}$ is the algebraic closure. It is a separable extension, so $n = [V : T]_s = [V : T]$.

We look for γ in the form $\gamma = \alpha + t\beta$ for some $t \in T$. If we know that $f_i(\alpha + t\beta) \neq f_j(\alpha + t\beta)$ for all $i \neq j$, then

$$n = [V : T] \geq [T(\gamma) : T] = [T(\gamma) : T]_s \underset{f_1, \dots, f_n \text{ are distinct}}{\geq} n.$$

So we have equalities everywhere, hence $V = T(\gamma)$.

How to choose t ? We want

$$\prod_{i < j} [f_j(\alpha + t\beta) - f_i(\alpha + t\beta)] = \prod_{i < j} [f_j(\alpha) - f_i(\alpha) + t(f_j(\beta) - f_i(\beta))] \neq 0.$$

For this it suffices that we have distinct ordered pairs $(f_i(\alpha), f_i(\beta)) \neq (f_j(\alpha), f_j(\beta))$ for all $i \neq j$, because then it is a nonzero polynomial and that has finitely many roots, so there is $t \in T$ which is not its root. But $f_i : T(\alpha, \beta) \rightarrow \bar{T}$ is uniquely determined by the values $f_i(\alpha), f_i(\beta)$, and hence the ordered pairs of these values for $i \neq j$ are indeed distinct. $\square$

Definition. Let U be a field.

$$\text{Aut}(U) := \{\varphi : U \rightarrow U \text{ automorphism}\}.$$

If G is a subgroup of $\text{Aut}(U)$, we define

$$\text{Fix}(U, G) = U^G := \{u \in U \mid g(u) = u \ \forall g \in G\}.$$

Remark. $\text{Fix}(U, G)$ is a field and $\text{Gal}(U/T)$ is a subgroup of the group $\text{Aut}(U)$ (for a field extension $U \supset T$).

The following theorem will be quite fundamental for the proof of the relationship between Gal and Fix in the Galois correspondence (Propositions 2.27, 2.28).

Theorem 2.21 (key theorem for the proof of the Galois correspondence). *Let us have a field U and a subgroup $G \subset \text{Aut}(U)$ of finite order n . Let $T = \text{Fix}(U, G)$. Then*

- a) $U \supset T$ is a separable extension,
- b) $[U : T] = n$,
- c) $\text{Gal}(U/T) = G$.

Proof. a) Let $\alpha \in U$. We want to prove that α is a root of some separable polynomial from $T[x]$. Consider $G\alpha := \{g\alpha \mid g \in G\}$ (which is the orbit of the element α under the action of G on U). Note that we have $g \in G \subset \text{Aut}(U)$, so g is an automorphism on U and $g\alpha = g(\alpha)$ is the image of the element $\alpha \in U$ under this automorphism (so in the notation $g\alpha$ we do not write parentheses around the element α).

Since $\text{id} \in G$, we have $\alpha \in G\alpha$. Let

$$f_\alpha(x) = \prod_{\beta \in G\alpha} (x - \beta).$$

We see that α is a root of f_α , the polynomial f_α is separable and $\deg f_\alpha \leq n = \#G$.

We want to prove that $f_\alpha \in T[x]$.

Recall that for $h \in \text{Aut}(U)$ and $f \in U[x]$ we define $h_x(f(x)) := \sum h(a_i)x^i$, where $f(x) = \sum a_i x^i$.

Let $h \in G$. Note that $h(G\alpha) := \{h\beta \mid \beta \in G\alpha\} = \{(hg)\alpha \mid g \in G\} = G\alpha$, i.e. h gives a permutation of the set $G\alpha$.

Hence

$$h_x(f_\alpha(x)) = \prod_{\beta \in G\alpha} (x - h\beta) = \prod_{\gamma \in G\alpha = h(G\alpha)} (x - \gamma) = f_\alpha(x).$$

We see that h fixes all coefficients of the polynomial f_α . This holds for all h , so $f_\alpha \in T[x]$, which is what we wanted to prove. Moreover, the degree of α as an algebraic element over T is $\leq n$.

b), c) First we prove that $[U : T] \leq n$. Suppose for a contradiction that $[U : T] > n$ (this degree could be finite or infinite). Then there is $U \supset V \supset T$ such that $[V : T] = k$ with $n < k < \infty$. But $U \supset T$ separable $\Rightarrow V \supset T$ separable.

By Theorem 2.20 there is then $\gamma \in V \subset U$ such that $V = T(\gamma)$. But then $n < k = [V : T] =$ the degree of γ over $T \leq n$ by the first part of the proof, which is a contradiction.

So we know that $[U : T] \leq n$. For $\varphi \in \text{Gal}(U/T)$ we have that $\varphi: U \rightarrow U$ is a T -automorphism. Hence φ gives a T -homomorphism $\varphi: U \rightarrow \bar{T}$ and we have

$$n = \#G \stackrel{G \subset \text{Gal}(U/T)}{\leq} \# \text{Gal}(U/T) \leq [U : T]_s \stackrel{2.16}{=} [U : T] \leq n.$$

So there must be equalities everywhere, and we have $G = \text{Gal}(U/T)$ and $[U : T] = n$. $\square$

2.9 Normal extensions

Definition. Let us have fields $T \subset U \subset \bar{T} =$ the algebraic closure of T . We say that U is a *normal extension* of T if it is an algebraic extension such that for every T -homomorphism $\varphi: U \rightarrow \bar{T}$ we have $\varphi(U) \subset U$, i.e. φ gives a T -homomorphism $U \rightarrow U$.

Recall that here we work with algebraic extensions, so $\bar{T} = \bar{U}$. We will thus not distinguish between these algebraic closures any further.

Definition. A *Galois extension* is a normal, separable extension of finite degree.

The following proposition gives an important intuition for normal extensions: they correspond to splitting fields.

Proposition 2.22.

- a) The splitting field of a polynomial f over T is a normal extension.
- b) The splitting field of a separable polynomial f over T is a Galois extension of T .
- c) Every Galois extension $U \supset T$ is the splitting field of some irreducible separable polynomial.

Proof. a) Let $U \subset \bar{T}$ be the splitting field of f over T . Let $\alpha_1, \dots, \alpha_n$ be the roots of f in U and let $\varphi: U \rightarrow \bar{T}$ be a T -homomorphism $\Rightarrow \varphi$ permutes $\{\alpha_1, \dots, \alpha_n\}$ by Proposition 2.12.

It is a splitting field, so $U = T(\alpha_1, \dots, \alpha_n)$, and hence φ is uniquely determined by the values $\varphi(\alpha_1), \dots, \varphi(\alpha_n)$, and these all lie in U . Therefore φ maps every element of $U = T(\alpha_1, \dots, \alpha_n)$ into U .

Clearly $U \supset T$ is algebraic, so it is indeed a normal extension.

b) f a separable polynomial $\Rightarrow \alpha_1, \dots, \alpha_n$ separable elements $\Rightarrow U = T(\alpha_1, \dots, \alpha_n)$ is a separable extension by 2.16. The finite degree is clear and we know normality from part a).

c) By Theorem 2.20, U is simple, i.e. $U = T(\gamma)$ for some γ .

Let f be the minimal polynomial of γ over T and let $\beta \in \bar{T}$ be a root of f . We want to prove that $\beta \in U$. By Lemma 2.5 we have a T -homomorphism

$$\begin{aligned} \varphi: T(\gamma) &\rightarrow T(\beta) \subset \bar{T} \\ \gamma &\mapsto \beta \end{aligned}$$

$U \supset T$ is normal, so $T(\beta) = \varphi(U) \subset U$, and hence $\beta \in U$.

We see that f splits in U into linear factors and $U = T(\gamma)$, so U is the splitting field of f .

f the minimal polynomial of $\gamma \Rightarrow f$ irreducible.

$U \supset T$ a separable extension $\Rightarrow \gamma$ a separable element $\Rightarrow f$ a separable polynomial. $\square$

Similarly as in part c) one shows the following useful lemma.

Lemma 2.23. *Let $U \supset T$ be a normal extension and $f \in T[x]$ irreducible. If f has one root in U , then it already has all its roots there.*

Proof. Let $\alpha \in U$ be a root of f and let $\beta \in \bar{T}$ be a root of f . By Lemma 2.5 we have a T -homomorphism

$$\begin{aligned} \varphi: T(\alpha) &\rightarrow T(\beta) \subset \bar{T} \\ \alpha &\mapsto \beta \end{aligned}$$

Using Corollary 2.11b) we extend φ to a T -homomorphism $\sigma: U \rightarrow \bar{T}$ such that $\sigma \upharpoonright T(\alpha) = \varphi$. $U \supset T$ normal, so $\sigma(U) \subset U$. This means that $\beta = \varphi(\alpha) = \sigma(\alpha) \in \sigma(U) \subset U$, as we wanted to prove. $\square$

Normal extensions can even be characterized as splitting fields; these are, however, splitting fields of sets of polynomials in the sense of the following definition.

Definition. $U \supset T$ is the *splitting field* of a set of polynomials $\mathcal{M} \subset T[x]$ if every polynomial $f \in \mathcal{M}$ splits in U into linear factors and $U = T[M]$, where M is the set of all roots of all polynomials $f \in \mathcal{M}$.

Proposition 2.24. *An extension $U \supset T$ is normal if and only if there is $\mathcal{M} \subset T[x]$ such that U is the splitting field of $\mathcal{M}$ over T .*

Proof. We only sketch the proof (for details see [Drápal, Proposition II.3.5]).

“ $\Rightarrow$ ” Define $\mathcal{M} := \{\text{the minimal polynomial of some } \alpha \in U\}$ and use Lemma 2.23.

“ $\Leftarrow$ ” Exercise (similarly as in Proposition 2.22a)). $\square$

Proposition 2.25.

Let $U \supset T$ be an extension and $V := \left\{ \alpha \in U \mid \begin{array}{l} \alpha \text{ algebraic over } T \text{ and the minimal polynomial} \\ \text{of } \alpha \text{ splits in } U \text{ into linear factors} \end{array} \right\}$.

Then V is a field which is the largest normal extension of T contained in U .

V is called the “normal closure of T in U ”.

Proof. Exercise (for a proof see [Drápal, Proposition II.3.6]). $\square$

2.10 Galois correspondence

We finally come to the mutually inverse relationship between the maps Fix and Gal .

The following proposition will be useful to us several times:

Proposition 2.26. *Let us have an algebraic field extension $U \supset T$ and a T -homomorphism $\varphi: U \rightarrow U$. Then φ is even a T -automorphism.*

Proof. We need to prove that φ is injective and onto.

Injective: $\text{Ker}(\varphi)$ is an ideal in the field U , and hence $\text{Ker}(\varphi) = 0, U$. Since φ is a T -homomorphism, we have $T \not\subset \text{Ker}(\varphi)$, and hence $\text{Ker}(\varphi) \neq U$. Therefore $\text{Ker}(\varphi) = 0$.

Onto: Let $\alpha \in U$. Since we are in an algebraic extension, there is a minimal polynomial $f(x) \in T[x]$ of α . By Proposition 2.12b), φ then gives a permutation of the set of roots of this polynomial in U , so there is a root β of the polynomial f such that $\varphi(\beta) = \alpha$. $\square$

Proposition 2.27. *Let $U \supset T$ be a field extension. Then:*

- a) $\text{Fix}(U, \text{Gal}(U/T)) \supset T$.
- b) For $G < \text{Aut}(U)$ we have $\text{Gal}(U/\text{Fix}(U, G)) \supset G$.
- c) If $U \supset T$ is a Galois extension, then

$$[U : T] = \# \text{Gal}(U/T) \text{ and } \text{Fix}(U, \text{Gal}(U/T)) = T.$$

Proof. a) Let $t \in T$. Then $\varphi(t) = t$ for every $\varphi \in \text{Gal}(U/T)$, because φ is a T -homomorphism. But this implies that $t \in \text{Fix}(U, \text{Gal}(U/T))$.

b) Similarly, it follows by writing out the definitions.

c) Let $S := \text{Fix}(U, \text{Gal}(U/T))$. By a) we have $S \supset T$. So it suffices to prove $[U : S] = [U : T]$ (because then $S = T$).

The extension $U \supset T$ is normal, so

$$\begin{aligned} [U : T]_s &= \#\{\varphi : U \rightarrow \bar{T} \mid T\text{-hom}\} \stackrel{\text{normal}}{=} \#\{\varphi : U \rightarrow U \mid T\text{-hom}\} \\ &\stackrel{2.26}{=} \#\{\varphi : U \rightarrow U \mid T\text{-automorphism}\} = \# \text{Gal}(U/T). \end{aligned}$$

The extension $U \supset T$ is separable, so $[U : T]_s = [U : T]$.

The group $\text{Gal}(U/T)$ is finite, because we have proved that $\# \text{Gal}(U/T) = [U : T]_s = [U : T]$. So we can use Theorem 2.21 for U and $G = \text{Gal}(U/T)$. For $S = \text{Fix}(U, G)$ it gives $[U : S] = \#G$ and $\text{Gal}(U/S) = G$. Hence $[U : S] = \# \text{Gal}(U/T)$.

Altogether we have $[U : T] = [U : S]$, as we wanted. $\square$

Definition. Let us have (partially) ordered sets $(A, \leq)$ and $(B, \leq)$ and maps $\alpha : A \rightarrow B, \beta : B \rightarrow A$ such that:

$$a_1 \leq a_2 \Rightarrow \alpha(a_1) \geq \alpha(a_2),$$

$$b_1 \leq b_2 \Rightarrow \beta(b_1) \geq \beta(b_2),$$

$$a \leq \beta(\alpha(a)), b \leq \alpha(\beta(b)).$$

Then (α, β) is called an (abstract) Galois correspondence between A and B .

Example. Let $U \supset T$ be a field extension and consider the sets, ordered by inclusion,

$$A := \{\text{fields } V \mid T \subset V \subset U\} \text{ and } B := \{\text{subgroups } G < \text{Gal}(U/T)\}.$$

As the maps from the definition we can then take

$$\alpha(V) = \text{Gal}(U/V) \text{ and } \beta(G) = \text{Fix}(U, G).$$

By Proposition 2.27a), b) this is a Galois correspondence.

We will see another example of a Galois correspondence in the next chapter on algebraic geometry.

Proposition 2.28. *Let (α, β) be an abstract Galois correspondence.*

- a) *Then α, β provide mutually inverse bijections between $\text{Im } \alpha$ and $\text{Im } \beta$.*
- b) *If α, β are surjective, then they are bijective and give mutually inverse anti-isomorphisms of the ordered sets $(A, \leq)$ and $(B, \leq)$.*

Similarly in case b), if moreover $(A, \leq)$ and $(B, \leq)$ are lattices, then α, β give mutually inverse anti-isomorphisms of these lattices.

Proof. a) For $a \in A$ we have $\beta\alpha a \geq a$, and hence $\alpha(\beta\alpha a) \leq \alpha a$.

At the same time $\alpha\beta(\alpha a) \geq \alpha a$; altogether we thus have $\alpha\beta\alpha a = \alpha a$.

So the composition $\alpha\beta: \text{Im } \alpha \rightarrow \text{Im } \alpha$ is the identity.

This composition is $\text{Im } \alpha \xrightarrow{\beta} \text{Im } \beta \xrightarrow{\alpha} \text{Im } \alpha$, and hence necessarily $\alpha: \text{Im } \beta \rightarrow \text{Im } \alpha$ is onto and $\beta: \text{Im } \alpha \rightarrow \text{Im } \beta$ is injective.

Symmetrically: $\alpha: \text{Im } \beta \rightarrow \text{Im } \alpha$ is injective and $\beta: \text{Im } \alpha \rightarrow \text{Im } \beta$ is onto. Hence α, β are bijections on the images $\text{Im } \alpha, \text{Im } \beta$.

b) is clear, because α, β reverse the ordering by definition. $\square$

Theorem 2.29 (Fundamental theorem of Galois theory). *Let $U \supset T$ be a Galois extension. Then we have an anti-isomorphism of ordered sets*

$$\begin{aligned} \{\text{field } V \mid T \subset V \subset U\} &\longleftrightarrow \{\text{subgroups } H < \text{Gal}(U/T)\} \\ V &\longmapsto \text{Gal}(U/V) \\ \text{Fix}(U, H) &\longleftarrow H \end{aligned}$$

Normal extensions of the field T correspond to normal subgroups of $\text{Gal}(U/T)$.

Proof. By Proposition 2.27 this is a Galois correspondence. Theorem 2.21 implies that the map $V \mapsto \text{Gal}(U/V)$ is surjective.

Let $T \subset V \subset U$. Then $U \supset V$ is also a Galois extension (exercise!), so we can use Proposition 2.27c). By it, $V = \text{Fix}(U, \text{Gal}(U/V))$, and hence $H \mapsto \text{Fix}(U, H)$ is onto. Proposition 2.28b) then gives the anti-isomorphism.

It remains to prove the part about normal extensions, for which we prove two implications.

1. Let $V \supset T$ be normal. Consider $\varphi \in \text{Gal}(U/T)$, i.e. a T -automorphism $\varphi: U \rightarrow U$. By its restriction to V we get a T -homomorphism $\varphi \upharpoonright V: V \rightarrow U \subset \bar{T}$. But $V \supset T$ is normal, so the image of this restriction lies in V , i.e. $\varphi \upharpoonright V: V \rightarrow V$. By Proposition 2.26 it is then an automorphism, i.e. $\varphi(V) = V$.

Let $\psi \in \text{Gal}(U/V)$; to prove the normality of this subgroup we want to prove that $\varphi\psi\varphi^{-1} \in \text{Gal}(U/V) < \text{Gal}(U/T)$, i.e. we want $\varphi\psi\varphi^{-1}(v) = v$ for every $v \in V$.

Since $\varphi(V) = V$, we have $\varphi^{-1}(v) \in V$. Hence $\psi\varphi^{-1}(v) = \varphi^{-1}(v)$ and

$$\varphi\psi\varphi^{-1}(v) = \varphi\varphi^{-1}(v) = v.$$

Hence $\text{Gal}(U/V)$ is a normal subgroup of $\text{Gal}(U/T)$.

2. Let $H \triangleleft \text{Gal}(U/T)$ be a normal subgroup. The following observation will be useful:

Exercise. Let U be a field and $G < \text{Aut}(U)$ a subgroup. Then for all $\varphi \in \text{Aut}(U)$ we have $\text{Fix}(U, \varphi G \varphi^{-1}) = \varphi(\text{Fix}(U, G))$ (where $\varphi G \varphi^{-1} = \{\varphi g \varphi^{-1} \mid g \in G\}$).

By this exercise, for $\varphi \in \text{Gal}(U/T)$ we thus have $\text{Fix}(U, \varphi H \varphi^{-1}) = \varphi(\text{Fix}(U, H))$. At the same time, by normality $\varphi H \varphi^{-1} = H$, so $\text{Fix}(U, H) = \text{Fix}(U, \varphi H \varphi^{-1}) = \varphi(\text{Fix}(U, H))$.

So we have proved:

⊗ every $\varphi \in \text{Gal}(U/T)$ maps $V = \text{Fix}(U, H)$ onto itself.

Let us now finally prove that $V \supset T$ is a normal extension. Let $\varphi: V \rightarrow \bar{T} (= \bar{U} = \bar{V})$ be a T -homomorphism. By Corollary 2.11b), φ can be extended to a T -homomorphism $\psi: U \rightarrow \bar{T}$.

The extension $U \supset T$ is normal, so $\psi(U) \subset U$. By Proposition 2.26, $\psi \in \text{Gal}(U/T)$.

At the same time $\varphi = \psi \upharpoonright V$. By ⊗ we have $\psi(V) = V$, and hence $\varphi(V) = V$.

Hence $V \supset T$ is a normal extension. $\square$

Corollary 2.30. *Let us have fields $U \supset V \supset T$ such that $U \supset T$ and $V \supset T$ are Galois extensions. Then*

$$\text{Gal}(U/T)/\text{Gal}(U/V) \simeq \text{Gal}(V/T).$$

Proof. Consider the map

$$\Phi : \text{Gal}(U/T) \rightarrow \text{Gal}(V/T), \varphi \mapsto \varphi|_V.$$

By item 1. in the previous proof we know that Φ is a well-defined map; clearly it is a homomorphism. We also see that $\text{Ker } \Phi = \text{Gal}(U/V)$, because the kernel consists exactly of those automorphisms of the field U whose restriction to V is the identity. By Corollary 2.11b, every element of $\text{Gal}(V/T)$ can be extended to an element of $\text{Gal}(U/T)$ (the extension maps U into U by normality and is an automorphism by Proposition 2.26), i.e. Φ is surjective. The 1st isomorphism theorem then gives the desired isomorphism (and also an alternative proof of the fact that $\text{Gal}(U/V) \triangleleft \text{Gal}(U/T)$). $\square$

2.11 Computations of Galois groups

Example. $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \simeq \mathbb{Z}/2$

Theorem 2.31. *Let $n \in \mathbb{N}$, $a_1, \dots, a_n \in \mathbb{Q}$ be such that for every non-empty subset $I \subset \{1, \dots, n\}$ we have $\prod_{i \in I} \sqrt{a_i} \notin \mathbb{Q}$. Then:*

- $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}) \supset \mathbb{Q}$ is a Galois extension
- $[\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}) : \mathbb{Q}] = 2^n$.
- $\text{Gal}(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})/\mathbb{Q}) \simeq (\mathbb{Z}/2)^n$

Remark. Instead of $\mathbb{Q}$ we can take any T of characteristic $\neq 2$.

Proof. Let $K := \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$. The key to the proof is to prove that $[K : \mathbb{Q}] = 2^n$. For a proof of this fact see the text by Jan Šároch *Lineárni nezávislost druhých odmocnin* [Linear independence of square roots], <http://karlin.mff.cuni.cz/~kala/1819%20ko/odm.pdf>.

Here we only indicate how the rest of the proof easily follows from it.

So assume that $[K : \mathbb{Q}] = 2^n$. The extension $K \supset \mathbb{Q}$ is of finite degree, separable and normal (it is indeed the splitting field of the polynomial $(x^2 - a_1) \cdots (x^2 - a_n)$), and hence $\#\text{Gal}(K/\mathbb{Q}) = [K : \mathbb{Q}] = 2^n$.

Every automorphism $\varphi \in \text{Gal}(K/\mathbb{Q})$ is determined by its values on $\sqrt{a_1}, \dots, \sqrt{a_n}$ and $\varphi(\sqrt{a_i}) = \pm\sqrt{a_i}$. There are thus at most 2^n such φ .

At the same time $\#\text{Gal}(K/\mathbb{Q}) = 2^n$, so each of the combinations of signs indeed gives an element of $\text{Gal}(K/\mathbb{Q})$. Each choice of the sign for $\sqrt{a_i}$ corresponds to one component $\mathbb{Z}/2$, so $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2)^n$ (here, of course, one has to think carefully about why this is an isomorphism of groups – and what it actually looks like!). $\square$

Similarly, when determining other Galois groups, the hardest step is often to determine the degree of the given extension. For example, for the cyclotomic fields $\mathbb{Q}(e^{2\pi i/n}) \supset \mathbb{Q}$ the degree of the extension is given by Euler's function $\varphi(n)$. The proof of this fact relies on the proof of the irreducibility of cyclotomic polynomials, which is fairly nontrivial (see the second-year lecture Number Theory and my lecture notes for it). From this it is then easy to prove (similarly as in the partial proof of Theorem 2.31 above) that

$$\text{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \simeq (\mathbb{Z}/n)^\times,$$

where the element $a \in (\mathbb{Z}/n)^\times$ corresponds to the automorphism $e^{2\pi i/n} \mapsto e^{2\pi ia/n}$.

3. Algebraic geometry

3.1 Algebraic sets and ideals

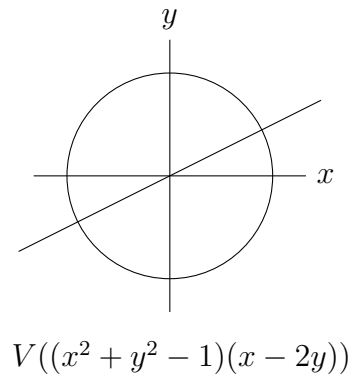
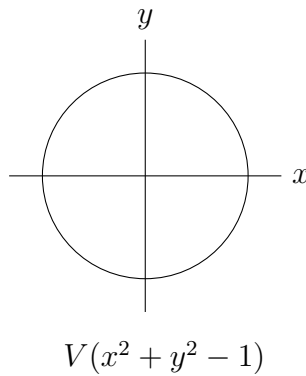
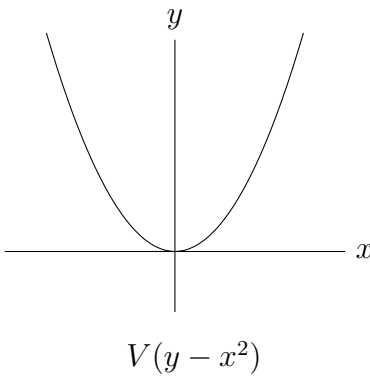
- K = a field (sometimes algebraically closed)
- $R = K[x_1, \dots, x_n]$

Definition. Let $p = (a_1, \dots, a_n) \in K^n$ and $f \in K[x_1, \dots, x_n]$. The point p is a *zero* of the polynomial f if $f(p) = 0$.

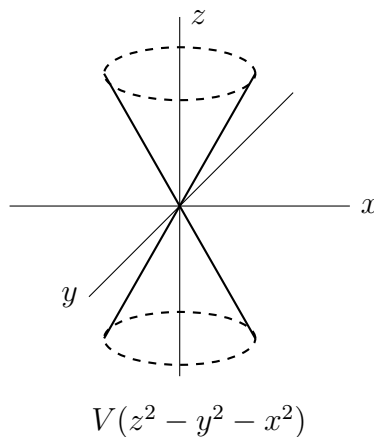
The set of all zeros of the polynomial f is denoted $V(f)$. If f is not a constant polynomial, then $V(f)$ is called a *hypersurface*.

Example.

- $n = 2$:



- $n = 3$: a cone



- $y = e^x$ is not a hypersurface

Definition. For a set of polynomials $S \subset K[x_1, \dots, x_n]$ we define

$$V(S) = \{p \in K^n \mid f(p) = 0 \forall f \in S\}.$$

A set $X \subset K^n$ is an *algebraic set* if $X = V(S)$ for some $S \subset K[x_1, \dots, x_n]$.

Clearly $S \subset S' \Rightarrow V(S) \supset V(S')$ (but the converse implication need not hold!).

We have the following basic properties of the map V (recall that $R = K[x_1, \dots, x_n]$):

Lemma 3.1. *Let $I = (S)$ be the ideal generated by a set $S \subset R$ in the ring R . Then $V(I) = V(S)$.*

Proof. “ $\subseteq$ ”: Clear

“ $\supseteq$ ”: It suffices to write out how generating works: $I = \{\sum r_i f_i \mid r_i \in R, f_i \in S\}$ (finite sums). So if $f(p) = 0$ for all $f \in S$, then also $(\sum r_i f_i)(p) = 0$. $\square$

Hence every algebraic set is of the form $V(I)$ for some ideal $I < R$.

Lemma 3.2. *a) If $\mathcal{J}$ is a set of ideals in R , then*

$$V\left(\bigcup_{I \in \mathcal{J}} I\right) = \bigcap_{I \in \mathcal{J}} V(I).$$

An intersection of arbitrarily many algebraic sets is an algebraic set.

b) Let $f, g \in R$ and $I, J < R$. Then $V(fg) = V(f) \cup V(g)$ and

$$V(I) \cup V(J) = V(\{fg \mid f \in I, g \in J\}) = V(IJ).$$

A union of finitely many algebraic sets is an algebraic set.

c) $V(0) = K^n, V(1) = \emptyset$

$V((x_1 - a_1, \dots, x_n - a_n)) = \{(a_1, \dots, a_n)\} \forall (a_1, \dots, a_n) \in K^n$.

Every finite subset of K^n is algebraic.

Proof. An easy exercise. $\square$

Many common sets are algebraic; the aim of *algebraic geometry* is to understand their structure. For example, we have this surprising property:

Proposition 3.3. *Every algebraic set $X \subsetneq K^n$ is an intersection of finitely many hypersurfaces.*

Proof. Let $X = V(I)$ for an ideal $I < R$. Since $X \neq K^n$, we have $I \neq 0$.

Since K is a field, it is also a Noetherian ring. By Corollary 1.12 of Hilbert’s basis theorem, $R = K[x_1, \dots, x_n]$ is Noetherian as well. By Proposition 1.10 the ideal I is then finitely generated, i.e. $I = (f_1, \dots, f_k)$ for some polynomials $f_i \neq 0$.

Hence $X = V(I) = V(\{f_1, \dots, f_k\}) = \bigcap V(f_i)$.

We need the f_i to be non-constant, so that $X = \bigcap$ hypersurfaces $V(f_i)$.

If $f_i = c, c \neq 0$, for some i , then necessarily $1 \in I$ (because R contains c^{-1}). Then $I = R$, from which it follows that $X = V(I) = V(R) = \emptyset$. But for $X = \emptyset$ it suffices to choose for example $f(x_1, \dots, x_n) = x_1, g(x_1, \dots, x_n) = x_1 + 1$ and we get $V(f) \cap V(g) = \emptyset = X$. $\square$

Definition. For a set $X \subset K^n$ we define the *ideal of the set X* as

$$I(X) = \{f \in R \mid f(p) = 0 \forall p \in X\}.$$

(Clearly it is an ideal.)

Clearly we have $X \subset Y \Rightarrow I(X) \supset I(Y)$.

Proposition 3.4. a) $I(\emptyset) = R$.

b) $I(K^n) = 0$ if K is an infinite field.

c) $I(\{(a_1, \dots, a_n)\}) = (x_1 - a_1, \dots, x_n - a_n)$.

Surprisingly, it is not completely trivial to prove parts b) and c); b) need not hold over a finite field:

Example. Let $K = \mathbb{F}_p = \mathbb{Z}/p$.

By Fermat's little theorem we have $a^p = a$ for every $a \in K$, and hence all these elements are roots of $x^p - x \in I(K)$.

(In fact $I(K) = (x^p - x)$.)

Proof. a) is clear.

b) We want to prove that if $f(a_1, \dots, a_n) = 0$ for all $a_1, \dots, a_n \in K$, then $f = 0$. By induction on n :
 $n = 1$: a nonzero $f(x_1)$ has only finitely many roots, whereas K is infinite.

$n \geq 2$: Let

$$0 \neq f(x_1, \dots, x_n) = \sum_{i=0}^k f_i(x_1, \dots, x_{n-1})x_n^i \text{ for } f_i \in K[x_1, \dots, x_{n-1}].$$

Choose $a_1, \dots, a_{n-1} \in K$ and consider $f(a_1, \dots, a_{n-1}, x_n)$. We have 2 possibilities:

1) It is the zero polynomial (in the variable x_n). Then $(a_1, \dots, a_{n-1})$ is a zero of all f_i , but $f(x_1, \dots, x_n) \neq 0$, and hence some $f_i(x_1, \dots, x_{n-1}) \neq 0$. By the induction hypothesis this polynomial does not have all $(a_1, \dots, a_{n-1}) \in K^{n-1}$ as zeros, and hence there is $(a_1, \dots, a_{n-1}) \in K^{n-1}$ for which case 2) occurs:
 2) $f(a_1, \dots, a_{n-1}, x_n)$ is a nonzero polynomial. It then has finitely many roots, and hence there are only finitely many a_n such that $f(a_1, \dots, a_{n-1}, a_n) = 0$. Hence $f \notin I(K^n)$.

c) Let us express the polynomial f by its "Taylor expansion around the point $(a_1, \dots, a_n)$ ", i.e.

$$f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n} \lambda_{i_1, \dots, i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n} \text{ for } \lambda_{i_1, \dots, i_n} \in K$$

(where only finitely many coefficients $\lambda_{i_1, \dots, i_n} \neq 0$).

Why is this possible? Consider the polynomial

$$f(y_1 + a_1, \dots, y_n + a_n) = g(y_1, \dots, y_n) = \sum \lambda_{i_1, \dots, i_n} y_1^{i_1} \cdots y_n^{i_n}.$$

Then we have $f(x_1, \dots, x_n) = g(x_1 - a_1, \dots, x_n - a_n)$, which gives the desired expression.

If $f \in I(\{(a_1, \dots, a_n)\})$, then $\lambda_{0, \dots, 0} = f(a_1, \dots, a_n) = 0$, and hence $f \in (x_1 - a_1, \dots, x_n - a_n)$. The opposite inclusion is clear. $\square$

Proposition 3.5. Let $S \subset R$ and $X \subset K^n$. Then:

a)

$$I(V(S)) \supset S, V(I(X)) \supset X$$

The maps I, V thus give an abstract Galois correspondence.

b)

$$V(I(V(S))) = V(S), I(V(I(X))) = I(X)$$

Proof. a) is easily verified by writing out the definitions.

b) then follows from Proposition 2.28. $\square$

What are the images of V and I ? The images of V are, by definition, the algebraic sets. If K is algebraically closed, then the images of I are the radical ideals (see the definition in the next section), as we will eventually prove.

3.2 Radicals

In this section let R be a general ring.

Definition. Let $I < R$ be an ideal. Then we define its *radical*

$$\sqrt{I} = \{a \in R \mid \exists k \geq 1 : a^k \in I\}.$$

An ideal I is *radical* if $I = \sqrt{I}$.

Observation. $\sqrt{I}$ is an ideal.

Proof. Let $a, b \in \sqrt{I}$. We want to check that $a + b \in \sqrt{I}$ ($ra \in \sqrt{I}$ for $r \in R$ is easy).

From the definition we have $a^k, b^l \in I$ and we compute

$$(a + b)^{k+l-1} = a^{k+l-1} + \binom{k+l-1}{1} a^{k+l-2}b + \dots + b^{k+l-1}.$$

Each of the first l summands is a multiple of $a^k \in I$ and each of the remaining k is a multiple of $b^l \in I$, so the whole sum lies in I and $a + b \in \sqrt{I}$. $\square$

Lemma 3.6. Let $X \subset K^n$. Then $I(X)$ is a radical ideal, i.e. $I(X) = \sqrt{I(X)}$

Proof. The inclusion “ $\subset$ ” is clear. For the opposite inclusion “ $\supset$ ” let $f \in \sqrt{I(X)}$. Then $f^k \in I(X)$ for some k , which means that $f^k(p) = 0$ for all $p \in X$. But this implies $f(p) = 0$, and hence $f \in I(X)$. $\square$

Definition. Let I be an ideal. The set of all prime ideals P in R which contain I is called the variety of I and is denoted $\text{Var } I$.

Exercise. If I is a proper ideal, then $\text{Var } I$ is non-empty.

Let us recall that a prime ideal is by definition a proper ideal.

Proposition 3.7. Let $I < R$ be a proper ideal and $P \in \text{Var } I$. Then $\text{Var } I$ contains at least one minimal element Q such that $Q \subset P$. That is, if $Q' \in \text{Var } I$ and $Q' \subset Q$, then $Q' = Q$.

Proof. We use Zorn’s lemma 1.23 on the set $\text{Var } I$ ordered by *reverse inclusion*, i.e. $Q_1 \leq Q_2 \Leftrightarrow Q_1 \supset Q_2$.

The empty chain has the upper bound P . Let us have a non-empty chain $\mathcal{B}$ in $\text{Var } I$. Does it have an upper bound? Let us try $\bigcap_{Q \in \mathcal{B}} Q$, which is clearly an ideal.

We have $Q \supset I$ for all $Q \in \text{Var } I$, and hence $\bigcap_{Q \in \mathcal{B}} Q \supset I$.

Is $\bigcap_{Q \in \mathcal{B}} Q =: J$ a prime ideal? Let $ab \in J, a \notin J$; we want to prove $b \in J$.

$a \notin J$, so there is $Q_0 \in \mathcal{B}$ such that $a \notin Q_0 \forall Q \subset Q_0$. But $ab \in J$, and hence $ab \in Q \forall Q \subset Q_0$. Q is a prime ideal, and therefore $b \in Q \forall Q \subset Q_0$.

But we have a chain, so $b \in Q \forall Q \in \mathcal{B}$, which already implies $b \in J$.

The hypotheses of Zorn’s lemma are satisfied, so there is a maximal element Q with respect to $\leq$ which is greater than P . This element Q is thus a minimal element with respect to $\subset$ and $Q \subset P$. $\square$

Proposition 3.8. Let I be a proper ideal in R . Then $\sqrt{I} = \bigcap_{P \in \text{Var } I} P$.

Proof. “ $\subset$ ”: Let $a \in \sqrt{I}$, $P \in \text{Var } I$. We want $a \in P$.

We have $a^k \in I \subset P$, and hence $a^k = a^{k-1}a \in P$. Then we have $a \in P$, as we wanted, or $a^{k-1} = a^{k-2}a \in P$, whence again $a \in P$ or $a^{k-2} \in P$ etc., until we get $a \in P$ in all cases.

“ $\supset$ ”: Let $b \in P \ \forall P \in \text{Var } I$. We want $b \in \sqrt{I}$. Suppose for a contradiction that $b \notin \sqrt{I}$ and let $S = \{b^k \mid k \geq 1\}$.

Recall that by Proposition 1.26, for every multiplicative set S and ideal $I < R$, $I \cap S = \emptyset$, there is $P \in \text{Var } I$ such that $P \cap S = \emptyset$.

S is closed under multiplication, moreover $0 \notin S$, because if it were, then $\exists k : b^k = 0 \in I$, and hence $b \in \sqrt{I}$.

Hence S is a multiplicative set and we can use Proposition 1.26: $b \notin \sqrt{I}$, so $I \cap S = \emptyset$, and hence there is $P \in \text{Var } I$ such that $P \cap S = \emptyset$. But then $b \notin P$, which is a contradiction. $\square$

Definition. The nilradical of R is the ideal $\sqrt{0}$.

We have $\sqrt{0} = \bigcap_{P \text{ prime ideal}} P$.

Definition. The Jacobson radical is $\mathcal{J}(R) = \bigcap_{M \text{ maximal}} M$.

Proposition 3.9. $a \in R$ lies in $\mathcal{J}(R)$ if and only if $1 - ra \in R^\times$ for all $r \in R$.

Proof. Exercise. $\square$

3.3 Finitely generated fields

To prove the relationship between the maps I, V and to describe the image of the map I , we will need a number of statements about the finite generation of fields as a ring and as a module.

For this we will use the following notions:

Definition. Let $S \supset R$ be a ring extension. We say that the extension is

1. *ring-finite* if there are $n \geq 1$ and elements $a_1, \dots, a_n \in S$ such that $S = R[a_1, \dots, a_n]$;
2. *module-finite* if S is finitely generated as an R -module, i.e. there are $n \geq 1$ and elements $a_1, \dots, a_n \in S$ such that $S = Ra_1 + \dots + Ra_n$.

In this terminology, recall Proposition 2.2, according to which for domains $R \subset S$ and $v \in S$ the following statements are equivalent:

1. v is integral over R ,
2. $R[v] \supset R$ is module-finite,
3. $\exists R'$ a domain, $R[v] \subset R' \subset S$ and $R' \supset R$ is module-finite.

Corollary 3.10. Let $K \subset L$ be fields, K algebraically closed. If $L \supset K$ is module-finite, then $L = K$.

Proof. Let $\alpha \in L$. Then $K \subset K[\alpha] \subset L$ and L is a finitely generated K -module, so α is an integral element. By Proposition 2.2 over K , α is a root of some polynomial, i.e. $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$ for some $a_i \in K$. This part of the proof was already in the second-year Algebra course as the statement that every field extension of finite degree is algebraic.

But K is algebraically closed, so $\alpha \in K$. $\square$

Lemma 3.11. Let K be a field and $n \geq 1$. Then $K(x_1, \dots, x_n) \supset K$ is not ring-finite (i.e. there are no $f_1, \dots, f_m \in K(x_1, \dots, x_n)$ such that $K(x_1, \dots, x_n) = K[f_1, \dots, f_m]$).

Proof. Suppose for a contradiction that they exist and let $f_i = \frac{p_i}{q_i}$, where $p_i, q_i \in K[x_1, \dots, x_n]$. Clearly at least one $f_i \notin K[x_1, \dots, x_n]$ (otherwise $K[f_1, \dots, f_m] \subset K[x_1, \dots, x_n]$, which does not contain x_1^{-1}), i.e. $\deg q_i \geq 1$.

Consider the element $\frac{1}{q_1 \cdots q_m + 1} \in K[f_1, \dots, f_m]$; so this element can be expressed as a polynomial in $f_1, \dots, f_m$. In this expression we get rid of the denominators by multiplying by $(q_1 \cdots q_m + 1)q_1^{r_1} \cdots q_m^{r_m}$, where the exponents r_i are sufficiently large. We thus get an equality of the form

$$q_1^{r_1} \cdots q_m^{r_m} = (q_1 \cdots q_m + 1) \cdot a \text{ for some } a \in K[x_1, \dots, x_n].$$

We are in the Gaussian ring $K[x_1, \dots, x_n]$, so we can take a prime factor $f \mid q_1 \cdots q_m + 1$ with $\deg f \geq 1$. Then $f \mid q_i$ for some i , and hence $f \mid 1$, which is a contradiction. $\square$

Exercise: R a Gaussian domain and K its field of fractions. If $u \in K$ is integral over R , then $u \in R$.

Corollary 3.12. *Let K be a field and $L = K(x)$. Then there is no $0 \neq f \in K(x)$ such that $\forall z \in L \exists n \geq 1 : f^n z$ is integral over $K[x]$.*

Proof. By contradiction. In the previous exercise choose $R = K[x]$, whose field of fractions is L . $f^n z \in K(x)$ is integral over R , so $f^n z \in K[x] = R$, and hence $z \in K[x, f^{-1}]$. But this holds for all $z \in L$, so $L = K(x) = K[x, f^{-1}]$, which contradicts Lemma 3.11. $\square$

Proposition 3.13. *Let us have fields $K \subset L$. Assume that $L \supset K$ is a ring-finite extension, i.e. $L = K[v_1, \dots, v_n]$ for some $v_1, \dots, v_n \in L$. Then $L \supset K$ is a module-finite extension.*

Proof. We proceed by induction on n .

$n = 1$: $L = K[v]$. We have 2 cases:

- a) v is algebraic over K , so v is integral and by Proposition 2.2, $L = K[v]$ is a finitely generated K -module.
- b) v is not algebraic over K , so $L = K[v] = K[x]$. But L is a field, so at the same time $L = K(x)$, which contradicts Lemma 3.11.

$n \geq 2$: Let $K_1 = K(v_1)$, so that $L = K_1[v_2, \dots, v_n]$. The induction hypothesis implies that L is a finitely generated K_1 -module. Again we distinguish two cases:

- a) v_1 is algebraic over K . Then $K_1 = K[v_1]$ is a finitely generated K -module and by Homework 3.4a), L is a finitely generated K -module.
- b) $v_1 = x$ is transcendental over K . L is a finitely generated K_1 -module, so by Proposition 2.2, $v_2, \dots, v_n$ are integral over K_1 .

So we have equalities $v_i^{n_i} + a_{i,n_i-1}v_i^{n_i-1} + \cdots + a_{i,0} = 0$ for $a_{ij} \in K_1$.

We multiply them by α^{n_i} , where $0 \neq \alpha \in K[x]$ is a common multiple of the denominators of all a_{ij} . We thus get

$$(\alpha v_i)^{n_i} + \alpha a_{i,n_i-1}(\alpha v_i)^{n_i-1} + \cdots + \alpha^{n_i} a_{i,0} = 0,$$

so the elements αv_i are integral over $K[x]$.

$L = K[x][v_2, \dots, v_n]$, so for every $z \in L$ there is n such that $\alpha^n z$ is a polynomial in $\alpha v_2, \dots, \alpha v_n$ with coefficients in $K[x]$. These are integral elements and integral elements form a ring, so $\alpha^n z$ is integral over $K[x]$. In particular this holds for $z \in K(x) \subset L$, which however contradicts Corollary 3.12 (note that $\alpha \in K[x] \subset K(x)$). Hence b) cannot occur; only case a) can occur, in which we have already proved the statement. $\square$

Corollary 3.14. *Let $K \subset L$ be fields and K algebraically closed. If $L \supset K$ is a ring-finite extension, then $L = K$.*

Proof. Proposition 3.13 + Corollary 3.10. $\square$

3.4 Hilbert's Nullstellensatz

Theorem 3.15 (Weak Nullstellensatz).

Let K be a field and $R = K[x_1, \dots, x_n]$. Then:

- a) The ideal $I = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ is maximal in R for all $\alpha_1, \dots, \alpha_n \in K$. Moreover, a polynomial $f \in R$ lies in this ideal if and only if $f(\alpha_1, \dots, \alpha_n) = 0$.
- b) If K is algebraically closed, then all maximal ideals in R are of the form $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in K$.

Proof.

a) Consider a polynomial $f \in R$ as a polynomial in the variable x_n over $K[x_1, \dots, x_{n-1}]$. We can write it as $f = a_n(x_n - \alpha_n) + b_{n-1}$, where $a_n \in R$ and $b_{n-1} \in K[x_1, \dots, x_{n-1}]$. Similarly $b_{n-1} = a_{n-1}(x_{n-1} - \alpha_{n-1}) + b_{n-2}$, until we gradually get

$$f = \sum_{i=1}^n a_i(x_i - \alpha_i) + b_0, \text{ for } a_i \in R, b_0 \in K.$$

We see that $\sum a_i(x_i - \alpha_i) \in I = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$. Hence:

“Moreover”: $f \in I \Leftrightarrow f - \sum_{i=1}^n a_i(x_i - \alpha_i) \in I \Leftrightarrow b_0 \in I \Leftrightarrow b_0 = f(\alpha_1, \dots, \alpha_n) = 0$ (note that $I \neq R$, since $1 \notin I$ by the same argument).

“Maximality”: Let $f \notin I$, i.e. $b_0 \neq 0$. Consider the ideal $I + (f)$. It contains $b_0 \in K^\times$, and hence $1 = b_0 b_0^{-1} \in I + (f)$ and $I + (f) = R$. Hence I is a maximal ideal.

b) Let M be a maximal ideal in R . Then $L = R/M$ is a field and moreover we can take K as a subfield of L , because we have the projection $\pi: R \twoheadrightarrow R/M$, whose restriction $\pi \upharpoonright K: K \rightarrow R/M$ is injective (because $\text{Ker}(\pi \upharpoonright K) = K \cap M = 0$).

But L is generated over K by the elements $x_1 + M, \dots, x_n + M$ as a ring. Corollary 3.14 $\Rightarrow L = K$. Hence

$$\begin{aligned} \pi \upharpoonright K: K &\rightarrow L = R/M \\ a &\mapsto a + M \end{aligned}$$

is an isomorphism, so in particular it is surjective.

Therefore for every i there is α_i such that $x_i + M = \alpha_i + M$. Hence $x_i - \alpha_i \in M$, so $(x_1 - \alpha_1, \dots, x_n - \alpha_n) \subset M$. But the ideal $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ is maximal by a), and hence it equals M . $\square$

In particular, we see that $V(I) \neq \emptyset$ for every proper ideal $I < R$ (if K is algebraically closed). Indeed, $I \subset M$ for some maximal ideal M , and then $V(I) \supset V(M) = \{(\alpha_1, \dots, \alpha_n)\}$.

Theorem 3.16 (Hilbert's Nullstellensatz). Let K be an algebraically closed field and I an ideal in $R = K[x_1, \dots, x_n]$. Then $I(V(I)) = \sqrt{I}$.

Proof. “ $\supset$ ”: exercise

“ $\subset$ ”: Let $g \in I(V(I))$; we want $g \in \sqrt{I}$.

Every ideal in the Noetherian ring R is finitely generated by Proposition 1.10. Hence $I = (f_1, \dots, f_r)$ for some polynomials $f_1, \dots, f_r \in R$.

Consider the ideal $J = (f_1, \dots, f_r, x_{n+1}g - 1) < K[x_1, \dots, x_{n+1}]$. Then $V(J) = \emptyset$, because:

If $f_1(\alpha) = \dots = f_r(\alpha) = 0$ for some $\alpha \in K^n$, then also $g(\alpha) = 0$. So if $(\alpha, \alpha_{n+1}) \in K^{n+1}$ is a zero of $f_1, \dots, f_r$, then $g(\alpha, \alpha_{n+1}) = g(\alpha) = 0$, and hence $\alpha_{n+1}g(\alpha, \alpha_{n+1}) - 1 = -1 \neq 0$, so $(\alpha, \alpha_{n+1}) \notin V(J)$.

Hence J is not a proper ideal thanks to the weak Nullstellensatz 3.15 (and the remark after it). So we have $J = K[x_1, \dots, x_{n+1}] \ni 1$, so $\exists a_i, b \in K[x_1, \dots, x_{n+1}]$ such that $1 = \sum a_i f_i + b(x_{n+1}g - 1)$.

Let us now work in the field $K(x_1, \dots, x_{n+1})$. Put $y = \frac{1}{x_{n+1}}$, i.e. $x_{n+1} = \frac{1}{y}$. After substituting into the expression for 1 we get some powers of y in the denominators, so let us multiply the equality by y^N to get rid of them. We thus get $\sum c_i f_i + d(g - y) = y^N$, where $c_i, d \in K[x_1, \dots, x_n, y]$. Here we finally substitute $y = g$ and we have $I \ni \sum c_i f_i + 0 = g^N$, hence $g \in \sqrt{I}$. $\square$

We have thus described the image of the map I , so from the abstract Galois correspondence 2.28 we get:

Corollary 3.17. *Let K be an algebraically closed field. If I is a radical ideal in $R = K[x_1, \dots, x_n]$ (i.e. $I = \sqrt{I}$), then $I(V(I)) = I$.*

Hence we have a bijection (or, more precisely, an anti-isomorphism of ordered sets)

$$\begin{aligned} \{\text{radical ideals in } R\} &\leftrightarrow \{\text{algebraic sets in } K^n\} \\ I &\mapsto V(I) \\ I(X) &\leftarrow X \end{aligned}$$

Maximal ideals correspond to points in K^n .

3.5 Irreducible algebraic sets

What do prime ideals correspond to in this correspondence?

Definition. Let K be a field. An algebraic set $V \subset K^n$ is *reducible* if $V = V_1 \cup V_2$ for some algebraic sets $V_1, V_2 \subset K^n$, $V_1 \neq V \neq V_2$. Otherwise V is *irreducible*.

Proposition 3.18. *A non-empty algebraic set V is irreducible if and only if $I(V)$ is a prime ideal.*

Proof. Homework 3.3 $\square$

Lemma 3.19. *a) Let $\mathcal{S}$ be a non-empty set of ideals in a Noetherian ring R . Then $\mathcal{S}$ has a maximal element, i.e. there is $I \in \mathcal{S}$ such that for every $J \in \mathcal{S}$ we have $I \subset J \Rightarrow I = J$.*

b) Every non-empty set of algebraic sets $\mathcal{T}$ in K^n has a minimal element.

Proof. a) By contradiction: Suppose it does not hold, i.e. for every $I \in \mathcal{S}$ there is $J \in \mathcal{S}$ such that $I \subsetneq J$.

Choose an arbitrary $I_1 \in \mathcal{S}$; then let $I_2 \in \mathcal{S}$ satisfy $I_1 \subsetneq I_2$. Similarly choose $I_2 \subsetneq I_3$, etc. (here we need to use the axiom of choice), which gives an infinite increasing chain of ideals in a Noetherian ring, which is a contradiction.

b) We consider $\mathcal{S} := \{I(V) \mid V \in \mathcal{T}\}$. If $I(V)$ is its maximal element, then V is a minimal element of $\mathcal{T}$. $\square$

Theorem 3.20. *Let $V \subset K^n$ be an algebraic set. Then there are uniquely determined algebraic sets $V_1, \dots, V_m$ such that V_i is irreducible, $V = V_1 \cup \dots \cup V_m$ and $V_i \not\subset V_j$ for $i \neq j$. The V_i are the irreducible components of the set V .*

Proof. Let $\mathcal{T} = \left\{ \text{algebraic sets } V \subset K^n \mid \begin{array}{l} V \text{ is not a union of finitely many} \\ \text{irreducible algebraic sets} \end{array} \right\}$.

Suppose for a contradiction that $\mathcal{T} \neq \emptyset$. By Lemma 3.19 it then has a minimal element V . V is not irreducible, so $V = V_1 \cup V_2$ for algebraic sets $V_1, V_2 \subsetneq V$. By the minimality of V we have $V_1, V_2 \notin \mathcal{T}$, and hence V_1, V_2 can be decomposed, so V can be decomposed as well, which is a contradiction.

Every V can thus be written as $V = V_1 \cup \dots \cup V_m$ for irreducible V_i . We may assume that the sets V_i are pairwise distinct, and we discard all V_i such that $\exists j \neq i : V_i \subset V_j$.

Uniqueness: Let $V = V_1 \cup \dots \cup V_m = W_1 \cup \dots \cup W_\ell$. Then $V_i = (V_i \cap W_1) \cup \dots \cup (V_i \cap W_\ell)$. This is an irreducible set, so there is $j = \sigma(i)$ such that $V_i = V_i \cap W_{\sigma(i)}$, i.e. $V_i \subset W_{\sigma(i)}$. Similarly there is k such that $W_{\sigma(i)} \subset V_k$. Hence $V_i \subset V_k$, so $i = k$ and $V_i = W_{\sigma(i)}$. Symmetrically $\forall j \exists \rho(j) : W_j = V_{\rho(j)}$. $\square$

Corollary 3.21. *Let K be an algebraically closed field. If I is a prime ideal, then $V(I)$ is irreducible. We have a bijection*

$$\{\text{prime ideals in } K[x_1, \dots, x_n]\} \leftrightarrow \{\text{irreducible algebraic sets in } K^n\}.$$

Proof. If I is a prime ideal, then $I = \sqrt{I} = I(V(I))$ by Hilbert's Nullstellensatz 3.16. By Proposition 3.18, the fact that $I(V(I))$ is a prime ideal then implies that $V(I)$ is irreducible. The rest of the corollary is clear. $\square$

Corollary 3.22. *Let K be an algebraically closed field and $f = f_1^{n_1} \dots f_r^{n_r} \in K[x_1, \dots, x_n]$ the irreducible factorization of a non-constant polynomial f (with pairwise non-associated f_i). Then $V(f) = V(f_1) \cup \dots \cup V(f_r)$ is the irreducible decomposition of $V(f)$ and $I(V(f)) = (f_1 \dots f_r)$. We have a bijection*

$$\left\{ \begin{array}{l} \text{irreducible non-constant polynomials in } K[x_1, \dots, x_n] \\ \text{up to a nonzero constant multiple} \end{array} \right\} \leftrightarrow \{\text{irreducible hypersurfaces in } K^n\}.$$

Proof. Exercise. $\square$

4. Algebraic number theory

4.1 Factorizations of Diophantine equations

Algebraic number theory studies the properties of *number fields*, i.e. extensions $K \supset \mathbb{Q}$ of finite degree. The motivation for its development was the effort to solve Diophantine equations, as we briefly sketch here. For much more information and many solved examples I recommend the master's thesis of Maroš Hrnčiar <http://karlin.mff.cuni.cz/~kala/theses/hrnciar.pdf>.

4.1.1 $x^2 + 1 = y^3$

Example. Find all integers x, y such that $x^2 + 1 = y^3$.

Solution. We factor the equation as $(x + i)(x - i) = y^3$ in $\mathbb{Z}[i]$.

We only briefly sketch the principle. One gradually proves:

1. $\gcd(x + i, x - i) = 1$
2. $x + i \parallel (a + bi)^3$ for $a, b \in \mathbb{Z}$.
3. $x + i = \varepsilon(a + bi)^3$, where $\varepsilon \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. So these 4 cases need to be distinguished; let us illustrate the rest of the solution only for $\varepsilon = 1$.
4. $x + i = 1 \cdot (a + bi)^3 = a^3 + 3a^2bi - 3ab^2 - b^3i$
5. $1 = \operatorname{Im}(x + i) = 3a^2b - b^3 = b(3a^2 - b^2)$
6. $a = 0, b = -1$
7. $x = \operatorname{Re}(x + i) = a^3 - 3ab^2$
8. $x = 0 \Rightarrow y = 1$
9. The other three cases turn out the same: in fact there was no need to distinguish them, because every unit (i.e. invertible element) is a cube, so the equation has the single solution $(0, 1)$.

Which properties of $\mathbb{Z}[i]$ did we use?

- the conjugation $\overline{a + bi} = a - bi$ is the nontrivial element of $\operatorname{Gal}(\mathbb{Q}(i)/\mathbb{Q})$
- $\alpha \mid \beta \Rightarrow \bar{\alpha} \mid \bar{\beta}$
- the norm $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$
- $\alpha \mid \beta \Rightarrow N\alpha \mid N\beta$
- the units $\mathbb{Z}[i]^\times$:
 $\alpha \in \mathbb{Z}[i]^\times \Leftrightarrow N\alpha = \pm 1$. Hence $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
- Gaussianity (in the step 1. $\Rightarrow$ 2.).

4.1.2 $x^2 + 5 = y^3$

Example. Find all integers x, y such that $x^2 + 5 = y^3$.

Solution. Again we factor as $(x + \sqrt{-5})(x - \sqrt{-5}) = y^3$ in $\mathbb{Z}[\sqrt{-5}]$.

Properties of $\mathbb{Z}[\sqrt{-5}]$:

- $(a + b\sqrt{-5})' = a - b\sqrt{-5}$
- $N\alpha = \alpha\alpha' = a^2 + 5b^2 \geq 0$
- $\alpha \in \mathbb{Z}[\sqrt{-5}]^\times \Leftrightarrow N\alpha = \pm 1 \Leftrightarrow \alpha = \pm 1$.
- Gaussianity? No!

For example $2 \cdot 3 = 6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, but $2, 3, 1 \pm \sqrt{-5}$ are (non-associated) irreducible elements. Let us show it on the example of 2:

Let $\alpha \mid 2, \alpha \nmid 1, \alpha \nmid 2$.

Then $N\alpha \mid N2 = 4 \Rightarrow N\alpha = 1, 2, 4$. Since α is not invertible, $N\alpha \neq 1$.

If $N\alpha = 4$, then $N(\frac{2}{\alpha}) = 1$, so $\frac{2}{\alpha}$ is a unit and $\alpha \parallel 2$.

$2 = N\alpha = a^2 + 5b^2$ is not possible, because no such integers a, b exist.

To solve the problem with non-unique factorizations, “ideal numbers” were introduced:

$A = (2, 1 + \sqrt{-5})$, where we think of the notation as a gcd

$A' = (2, 1 - \sqrt{-5})$

$B = (3, 1 + \sqrt{-5})$

$B' = (3, 1 - \sqrt{-5})$

Then it makes sense to consider that $2 = AA', 1 + \sqrt{-5} = AB, 1 - \sqrt{-5} = A'B', 3 = BB'$, so we have the unique factorization $6 = AA'BB'$.

Recall that in $\mathbb{Z}$ the gcd corresponds to the addition of ideals: $(\gcd(m, n)) = (m) + (n)$.

So let us consider $A = (2, 1 + \sqrt{-5}) = 2 \cdot \mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ as an ideal.

Multiplication of ideals then gives $A \cdot A' = (2), A \cdot A' \cdot B \cdot B' = (6)$.

Prime ideals correspond to prime factors, and indeed the following holds:

Theorem. *Every nonzero ideal in $\mathbb{Z}[\sqrt{-5}]$ can be uniquely factored into a product of prime ideals.*

Proof. Eventually, as a special case of Theorem 4.17. □

The group of ideals

The set of all nonzero ideals in $\mathbb{Z}[\sqrt{-5}]$ (and also more generally) with the operation of multiplication can be extended to a group similarly as the field of fractions is constructed: We consider formal fractions AB^{-1} for nonzero ideals A, B , where we identify (formally by defining the corresponding equivalence) AB^{-1} with CD^{-1} if and only if $AD = BC$.

On the resulting set $\mathcal{I} = \{AB^{-1} \mid A, B \text{ nonzero ideals}\}$ we define multiplication by $(AB^{-1}) \cdot (CD^{-1}) = (AC)(BD)^{-1}$, which gives the *group of ideals*.

Also, for $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ we have the principal ideals $(\alpha), (\beta)$.

We then define $\mathcal{P} = \{(\alpha) \cdot (\beta)^{-1} \mid \alpha, \beta \in \mathbb{Z}[\sqrt{-5}] \setminus \{0\}\}$ as a subgroup of $\mathcal{I}$.

We have: PID $\Leftrightarrow \mathcal{I} = \mathcal{P} \Leftrightarrow \mathcal{I}/\mathcal{P} = \{1\}$.

Also PID $\Rightarrow$ Gaussianity (which is what interests us for solving Diophantine equations).

So we define the *class group* as $\mathcal{Cl} := \mathcal{I}/\mathcal{P}$.

In general: $\mathcal{Cl}$ is always *finite*. (Its size measures “how bad the non-uniqueness of factorizations is”.)

For $\mathbb{Z}[\sqrt{-5}]$ we have $\mathcal{Cl} \simeq \mathbb{Z}/2$ and we can finally sketch the solution of our equation $(x + \sqrt{-5})(x - \sqrt{-5}) = y^3$.

(1) By computing with ideals we find that there is no prime ideal P which would divide both $x + \sqrt{-5}$ and $x - \sqrt{-5}$; these two elements (resp. their principal ideals) are thus coprime.

(2) Now consider the factorization into prime ideals in the equation $(x + \sqrt{-5})(x - \sqrt{-5}) = (y)^3$:
 $P_1^{k_1} \dots P_r^{k_r} Q_1^{l_1} \dots Q_s^{l_s} = R_1^{3m_1} \dots R_t^{3m_t}$.

By the coprimality in item (1) we have $P_i \neq Q_j$.

Hence the uniqueness of factorizations implies $3 \mid k_i, 3 \mid l_j$ for all i, j .

(3) Hence there is an ideal $A < \mathbb{Z}[\sqrt{-5}]$ such that $(x + \sqrt{-5}) = A^3$.

(4) This ideal is principal, i.e. $A \in \mathcal{P}$, because:

We know that $A^3 \in \mathcal{P}$ by (3).

At the same time $\#\mathcal{C}\ell = 2$, and hence $I^2 \in \mathcal{P}$ for any ideal I .

But for our ideal this implies $A = A^3 \cdot (A^2)^{-1} \in \mathcal{P}$.

(5) Let $A = (a + b\sqrt{-5})$. Then $x + \sqrt{-5} = \pm(a + b\sqrt{-5})^3$. This is easily finished by multiplying out and comparing the rational and irrational parts; it turns out that the given equation has no solution in $\mathbb{Z}$.

Similarly, mathematicians tried to prove Fermat's Last Theorem for the equation $x^p - y^p = z^p$:

$(x - y)(x - \zeta_p y) \dots (x - \zeta_p^{p-1} y)$, where $\zeta_p = e^{\frac{2\pi i}{p}} \rightsquigarrow \mathbb{Z}[\zeta_p]$.

4.2 Integral elements

Definition. A field K is a *number field* if it is an extension of $\mathbb{Q}$ of finite degree.

Example. $\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta_p), \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, where $\zeta_p = e^{\frac{2\pi i}{p}}$.

A suitable analogue of the integers in K are the integral elements (see Section 2.3).

Definition. The ring of all elements of the field K which are integral over $\mathbb{Z}$ is denoted $\mathcal{O}_K$.

Clearly: $\mathcal{O}_{\overline{\mathbb{Q}}} \cap K = \mathcal{O}_K$.

Lemma 4.1. Let K be a number field. For $\alpha \in K$ let $m_\alpha(x) \in \mathbb{Q}[x]$ be its minimal monic polynomial. Then $\alpha \in \mathcal{O}_K$ if and only if $m_\alpha \in \mathbb{Z}[x]$.

Proof. “ $\Leftarrow$ ”: Clear

“ $\Rightarrow$ ”: Let $f \in \mathbb{Z}[x]$ be monic such that $f(\alpha) = 0$. Then $m_\alpha \mid f$ in the ring $\mathbb{Q}[x]$, i.e. $f = m_\alpha \cdot g$ for some $g \in \mathbb{Q}[x]$. Hence g is also monic.

Let k, ℓ be the least common multiples of the denominators of the coefficients of the polynomials m_α, g . Then $km_\alpha, \ell g \in \mathbb{Z}[x]$ are primitive polynomials. By Theorem 1.14, $km_\alpha \cdot \ell g \in \mathbb{Z}[x]$ is primitive as well. But $km_\alpha \cdot \ell g = k\ell f$ and $f \in \mathbb{Z}[x]$, which is possible only if $k = \ell = 1$, and hence $m_\alpha \in \mathbb{Z}[x]$. $\square$

Corollary 4.2.

a) $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$

b) Every element $\alpha \in K$ can be written as $\frac{\beta}{n}$, where $\beta \in \mathcal{O}_K, n \in \mathbb{N}$.

Proof.

a) $\alpha \in \mathcal{O}_K \cap \mathbb{Q} \Leftrightarrow m_\alpha(x) = (x - \alpha) \in \mathbb{Z}[x] \Leftrightarrow \alpha \in \mathbb{Z}$.

b) Let $m_\alpha(x) = \sum_{i=0}^d a_i x^i$, where $a_d = 1$, and let n be the least common multiple of the denominators of the coefficients $a_i \in \mathbb{Q}$, i.e. $n \cdot m_\alpha \in \mathbb{Z}[x]$ and $n \cdot m_\alpha$ is primitive.

Then $\alpha = \frac{\beta}{n}$ for $\beta = n\alpha \in \mathcal{O}_K$, where $n\alpha \in \mathcal{O}_K$, because its minimal monic polynomial is $\sum_{i=0}^d a_i n^{d-i} x^i \in \mathbb{Z}[x]$. $\square$

Example. Consider the quadratic field $K = \mathbb{Q}(\sqrt{D})$ for a square-free integer $D \neq 0, 1$. Then m_α has degree ≤ 2 for all $\alpha \in K$.

For $\alpha = a + b\sqrt{D}$ (with $b \neq 0$) we have

$$m_\alpha(x) = (x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha \cdot \alpha' = x^2 - 2ax + (a^2 - Db^2),$$

where $\alpha' = a - b\sqrt{D}$.

Why is it the minimal polynomial of α ?

$\alpha \notin \mathbb{Q}$, and hence m_α has degree exactly 2. The polynomial $(x - \alpha)(x - \alpha') \in \mathbb{Q}[x]$ has α as a root and has degree 2, so it is indeed the minimal polynomial m_α .

The form of this polynomial can be conveniently used to determine the ring of integral elements, as we will see in the next section.

4.3 Norm and trace

Convention. For the whole rest of the chapter let $K = \mathbb{Q}(\sqrt{D})$, where $D \neq 0, 1$ is a square-free integer.

We will also often use the term “unit” for any invertible element of the ring $\mathcal{O}_K$.

Definition. We define the norm as the map

$$\begin{aligned} N &= N_{K/\mathbb{Q}}: K \rightarrow \mathbb{Q} \\ \alpha = a + b\sqrt{D} &\mapsto \alpha \cdot \alpha' = a^2 - b^2D \end{aligned}$$

where $\alpha' = a - b\sqrt{D}$.

Definition. We define the trace as the map

$$\begin{aligned} \text{Tr} &= \text{Tr}_{K/\mathbb{Q}}: K \rightarrow \mathbb{Q} \\ \alpha = a + b\sqrt{D} &\mapsto \alpha + \alpha' = 2a \end{aligned}$$

Observation.

- $\alpha \in \mathcal{O}_K \Leftrightarrow \text{Tr}(\alpha), N\alpha \in \mathbb{Z}$.
For $\alpha \in K \setminus \mathbb{Q}$ we proved it in the example above; for $\alpha \in \mathbb{Q}$ it is a simple exercise.
- $(\alpha\beta)' = \alpha'\beta'$, $(\alpha + \beta)' = \alpha' + \beta'$
- $N(\alpha\beta) = N\alpha \cdot N\beta$, because we can write it out as $(\alpha\beta)(\alpha\beta)' = (\alpha\alpha')(\beta\beta')$.
 $\text{Tr}(\alpha + \beta) = \text{Tr}(\alpha) + \text{Tr}(\beta)$ similarly.

Theorem 4.3. Let $D \neq 0, 1$ be square-free and $K = \mathbb{Q}(\sqrt{D})$. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{for } D \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{for } D \equiv 1 \pmod{4} \end{cases}$$

Proof. We prove the inclusion “ $\subset$ ”; we leave the opposite inclusion as an easy exercise.

Let $\alpha \in \mathcal{O}_K$, $\alpha = a + b\sqrt{D}$. Then the trace $\text{Tr}(\alpha) = 2a$ is an integer, and hence $a = c/2$ for $c \in \mathbb{Z}$. The norm is also an integer, i.e.

$$N\alpha = a^2 - b^2D = \frac{c^2 - 4b^2D}{4} \in \mathbb{Z}.$$

In particular we have $4b^2D = (2b)^2D \in \mathbb{Z}$.

The denominator of the rational number $(2b)^2$ is a square, which must divide D in order that $(2b)^2 D \in \mathbb{Z}$. But D is square-free, and hence this denominator is 1, i.e. $(2b)^2$ and $2b$ are in $\mathbb{Z}$. Let $b = \frac{d}{2}$ for $d \in \mathbb{Z}$. Then $N\alpha = \frac{c^2 - d^2 D}{4} \in \mathbb{Z}$ implies $c^2 \equiv d^2 D \pmod{4}$.

Note that since $4 \nmid D$, the numbers c and d have the same parity. So let us distinguish two cases:

- 1) c, d even. Then $a = \frac{c}{2}, b = \frac{d}{2} \in \mathbb{Z}$.
- 2) c, d odd. Then $1 \equiv c^2 \equiv d^2 D \equiv D \pmod{4}$, i.e. necessarily $D \equiv 1 \pmod{4}$.

Hence for $D \equiv 2, 3 \pmod{4}$ case 1) must occur, and hence $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$.

If $D \equiv 1 \pmod{4}$, it can also happen that c, d are both odd.

But then $\alpha = a + b\sqrt{D} = \left(\frac{c-1}{2} + \frac{d-1}{2}\sqrt{D}\right) + \frac{1+\sqrt{D}}{2}$. Since the first summand lies in $\mathbb{Z}[\sqrt{D}] \subset \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, we get $\alpha \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. $\square$

Proposition 4.4. $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid N\alpha = \pm 1\}$

Proof. “ $\subset$ ”: $\alpha \in \mathcal{O}_K^\times \Rightarrow \exists \beta : \alpha\beta = 1 \Rightarrow N(\alpha) \cdot N(\beta) = N(1) = 1$.

$N\alpha, N\beta \in \mathbb{Z} \Rightarrow N\alpha = \pm 1$

“ $\supset$ ”: $N\alpha = \pm 1 \Rightarrow \alpha \cdot \alpha' = \pm 1 \Rightarrow \pm\alpha'$ is the inverse of α . $\square$

Example. $K = \mathbb{Q}(\sqrt{D})$

- $D < 0 \Rightarrow a^2 + b^2(-D) = \pm 1 \Rightarrow$ finitely many units, typically just $\mathcal{O}_K^\times = \{\pm 1\}$. There are more units in only two cases, namely
 $\mathcal{O}_{\mathbb{Q}(i)}^\times = \{\pm 1, \pm i\}$.
 $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}^\times = \{e^{\frac{k\pi i}{3}} \mid k \in \{0, 1, 2, 3, 4, 5\}\}$
- $D > 0, D \equiv 2, 3 \pmod{4}$. This amounts to the solutions of Pell’s equation $x^2 - Dy^2 = \pm 1$, which has infinitely many solutions.
 For example, for $D = 2$ we have $\mathcal{O}_K^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$.
 (For $0 < D \equiv 1 \pmod{4}$ one needs to consider Pell’s equation $x^2 - Dy^2 = \pm 4$.)

4.4 Ideals

We do not have unique factorizations into products of irreducible elements. For example, in $\mathbb{Z}[\sqrt{-14}]$ we have

$$3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14}) \text{ and } 3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}),$$

and all of these are irreducible elements.

Instead, we will factor into products of prime ideals, as we already indicated in Section 4.1. To this end we first prove some basic properties of ideals.

As in the whole chapter, let $K = \mathbb{Q}(\sqrt{D})$ for a square-free $D \neq 0, 1$.

Proposition 4.5. *Every ideal in $\mathcal{O}_K$ is finitely generated, in fact by at most two generators.*

Proof. An ideal I in $\mathcal{O}_K$ is a subgroup $I(+)$ of $\mathcal{O}_K(+) \simeq \mathbb{Z}^2(+)$ by Theorem 4.3. But every subgroup of $\mathbb{Z}^2$ is isomorphic to $\mathbb{Z}^n$ for some $0 \leq n \leq 2$ (exercise). Hence $I(+) \simeq \mathbb{Z}^n(+)$, and so I has $n \leq 2$ generators as an abelian group. $\square$

Example. What does the isomorphism $\mathcal{O}_K(+) \simeq \mathbb{Z}^2(+)$ look like?

- a) $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. Then $a + b\sqrt{D} \mapsto (a, b) \in \mathbb{Z}^2$.
- b) $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Then $a + b\frac{1+\sqrt{D}}{2} \mapsto (a, b) \in \mathbb{Z}^2$.

Corollary 4.6. $\mathcal{O}_K$ is a Noetherian domain.

Proof. Proposition 1.10 + Proposition 4.5. □

Lemma 4.7. Let $I < \mathcal{O}_K$ be an ideal such that $I = (a_1, \dots, a_m)$ for $a_1, \dots, a_m \in \mathbb{Z}$. Then $I = (a)$ is principal (for some $a \in \mathbb{Z}$).

Proof. Let $a = \gcd(a_1, \dots, a_m)$ in $\mathbb{Z}$. Then $a \mid a_i$ in $\mathbb{Z}$, so $a \mid a_i$ in $\mathcal{O}_K$, and hence $a_i \in (a)$. But this holds for all i , and hence $I \subset (a)$.

On the other hand, Bézout's identity in $\mathbb{Z}$ gives the existence of elements $b_i \in \mathbb{Z}$ such that $a = a_1b_1 + \dots + a_mb_m \in I$, and hence $(a) \subset I$. □

Proposition 4.8. Let $I = (\alpha_1, \dots, \alpha_m), J = (\beta_1, \dots, \beta_l), \alpha_i, \beta_i \in \mathcal{O}_K$. Then:

- $I + J = (\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_l)$
- $I \cdot J = (\alpha_1\beta_1, \alpha_1\beta_2, \dots, \alpha_i\beta_j, \dots, \alpha_m\beta_l)$
- $I \subset J \Leftrightarrow$ every α_i is an $\mathcal{O}_K$ -linear combination of the β_j
- $I \cdot J = 0 \Leftrightarrow I = 0$ or $J = 0$

Proof. The first 3 items are clear from the definitions. The last one is not hard either:

“ $\Leftarrow$ ” Clear.

“ $\Rightarrow$ ” By contradiction. Let $0 \neq \alpha \in I, 0 \neq \beta \in J$. But then $\alpha \cdot \beta \in I \cdot J = 0$. This contradicts the fact that $\mathcal{O}_K$ is a domain (which holds because it is a subset of the field $\mathcal{O}_K \subset K$). □

Definition. Let I, J be ideals in $\mathcal{O}_K$. We say that I divides J , written $I \mid J$, if there is an ideal H such that $J = I \cdot H$.

Observation. For $\alpha, \beta \in \mathcal{O}_K$ we have $\alpha \mid \beta \Leftrightarrow (\alpha) \mid (\beta)$.

Proof.

“ $\Rightarrow$ ”: $\exists \gamma \in \mathcal{O}_K$ such that $\beta = \alpha\gamma \Rightarrow (\beta) = (\alpha\gamma) = (\alpha)(\gamma) \Rightarrow (\alpha) \mid (\beta)$

“ $\Leftarrow$ ”: $\beta \in (\beta) = (\alpha) \cdot H = \{\alpha i \mid i \in H\}$. Hence $\exists i \in H : \beta = \alpha \cdot i \Rightarrow \alpha \mid \beta$. □

Proposition 4.9. Let $\alpha \in \mathcal{O}_K, I = (\beta_1, \dots, \beta_m) < \mathcal{O}_K$. The following statements are equivalent:

- a) $(\alpha) \mid I$
- b) $\alpha \mid \beta_j$ for all j
- c) $(\alpha) \supset I$

Proof. “ $a \Rightarrow b$ ” Let $I = (\alpha)J = \{\alpha i \mid i \in J\}$ for some ideal J . Then α divides all elements of I , in particular the generators, i.e. $\alpha \mid \beta_j \forall j$.

“ $b \Leftrightarrow c$ ” $\alpha \mid \beta_j$ for all $j \Leftrightarrow \alpha$ divides all elements of $I \Leftrightarrow I \subset (\alpha)$.

“ $b \Rightarrow a$ ” Let $\beta_j = \alpha\gamma_j$ for some elements $\gamma_j \in \mathcal{O}_K$. Then

$$I = (\beta_1, \dots, \beta_m) = (\alpha\gamma_1, \dots, \alpha\gamma_m) = (\alpha) \cdot (\gamma_1, \dots, \gamma_m),$$

and hence $(\alpha) \mid I$. □

Theorem 4.10. For ideals $I, J < \mathcal{O}_K$ we have $I \mid J \Leftrightarrow I \supset J$.

Proof. If one of the ideals I, J is zero, the equivalence holds trivially. So let us further consider only nonzero ideals. For these we prove only “ $\Rightarrow$ ” for now; the other implication will come in the next section.

Let $J = I \cdot H$. Since $H \subset \mathcal{O}_K$, we have $J = I \cdot H \subset I \cdot \mathcal{O}_K = I$. □

4.5 Cancellation of ideals

Still let $K = \mathbb{Q}(\sqrt{D})$ for a square-free $D \neq 0, 1$.

Definition. Let $I < \mathcal{O}_K$ be an ideal. Its *conjugate ideal* is $I' = \{\alpha' \mid \alpha \in I\}$.

Observation. Clearly we have:

- $(\alpha_1, \dots, \alpha_m)' = (\alpha'_1, \dots, \alpha'_m)$
- $(IJ)' = I'J'$
- $I'' = I$

Proposition 4.11. *Let $I = (\alpha, \beta) < \mathcal{O}_K$. Then $II' = (N\alpha, \text{Tr}(\alpha\beta'), N\beta)$, and hence II' is a principal ideal.*

Proof. If $\alpha = 0$ or $\beta = 0$, then the statement holds.

Let $\alpha \neq 0 \neq \beta$. We have

$$II' = (\alpha, \beta)(\alpha', \beta') = (\alpha\alpha', \alpha\beta', \alpha'\beta, \beta\beta') = (N\alpha, \alpha\beta', \alpha'\beta, N\beta).$$

Note that $\text{Tr}(\alpha\beta') = \alpha\beta' + \alpha'\beta$, and hence $(N\alpha, \text{Tr}(\alpha\beta'), N\beta) \subset II'$.

It remains to prove the opposite inclusion, for which we need $\alpha\beta' \in (N\alpha, \text{Tr}(\alpha\beta'), N\beta)$.

Let $g = \gcd_{\mathbb{Z}}(N\alpha, \text{Tr}(\alpha\beta'), N\beta)$, i.e. $(g) = (N\alpha, \text{Tr}(\alpha\beta'), N\beta)$ (see the proof of Lemma 4.7).

So we want to prove that $\alpha\beta' \in (g)$, i.e. $\frac{\alpha\beta'}{g} \in \mathcal{O}_K$. For this it suffices that the norm and the trace of this element are $\in \mathbb{Z}$. We have:

$$\text{Tr}\left(\frac{\alpha\beta'}{g}\right) = \frac{\alpha\beta'}{g} + \frac{\alpha'\beta}{g} = \frac{\alpha\beta' + \alpha'\beta}{g} = \frac{\text{Tr}(\alpha\beta')}{g} \in \mathbb{Z}, \text{ because } g = \gcd(N\alpha, \text{Tr}(\alpha\beta'), N\beta).$$

$$N\left(\frac{\alpha\beta'}{g}\right) = \frac{\alpha\beta'}{g} \cdot \frac{\alpha'\beta}{g} = \frac{\alpha\alpha'}{g} \cdot \frac{\beta\beta'}{g} = \frac{N\alpha}{g} \cdot \frac{N\beta}{g} \in \mathbb{Z}.$$

We have thus proved that $\alpha\beta' \in (g) = (N\alpha, \text{Tr}(\alpha\beta'), N\beta)$.

Symmetrically $\alpha'\beta \in (N\alpha, \text{Tr}(\alpha\beta'), N\beta)$, and hence $II' \subset (N\alpha, \text{Tr}(\alpha\beta'), N\beta)$.

That II' is a principal ideal then follows from Lemma 4.7. □

Corollary 4.12. *If $I = (\alpha_1, \dots, \alpha_m) < \mathcal{O}_K$, then II' is the ideal generated by the elements $N\alpha_1, \dots, N\alpha_m$ and all the elements $\text{Tr}(\alpha_i\alpha'_j)$ for $1 \leq i < j \leq m$.*

Proof. We repeatedly use Proposition 4.11. □

Now we can prove that nonzero ideals can be cancelled.

Proposition 4.13. *Let $H, I, J < \mathcal{O}_K$ be ideals such that $H \neq 0$ and $HI = HJ$. Then $I = J$.*

Proof. We distinguish two cases:

a) H is principal, i.e. $H = (\alpha), \alpha \neq 0$. We have $HI = (\alpha)I = \{\alpha i \mid i \in I\}$ and also $HJ = (\alpha)J = \{\alpha j \mid j \in J\}$.

$\mathcal{O}_K$ is a domain, and hence $\alpha i = \alpha j$ implies $i = j$. Hence $I = J$.

b) H is a general ideal. By Proposition 4.11 we have $HH' = (g)$ for some g (and $g \neq 0$, since $H \neq 0$). Then

$$HI = HJ \Rightarrow HH'I = HH'J \Rightarrow (g)I = (g)J \xrightarrow{\text{part a)}} I = J. \quad \square$$

Now we can return to the proof of the harder implication in Theorem 4.10.

Proof of Theorem 4.10. “ $\Leftarrow$ ”: Let $I \supset J$. Then $II' \supset JJ'$. By Proposition 4.11 there is g such that $II' = (g)$.

So we have $(g) \supset JJ'$. By Proposition 4.9, $(g) \mid JJ'$, so there is an ideal H such that $JJ' = (g)H = II'H$. By Proposition 4.13 we can cancel I' , which gives $J = IH$, i.e. $I \mid J$. □

Let us note that while Theorem 4.10 holds in general (and is the key to the proof of unique factorization into prime ideals in Theorem 4.17), Proposition 4.11 is specific to quadratic fields only. In general, the proof of Theorem 4.10 works with “fractional ideals” and “annihilators”.

Corollary 4.14. *Let us have a prime ideal $P < \mathcal{O}_K$ and ideals $I, J < \mathcal{O}_K$. If $P \mid IJ$, then $P \mid I$ or $P \mid J$.*

Proof. $P \mid IJ \xrightarrow{4.10} P \supset IJ \xrightarrow{\text{def.}} P \supset I$ or $P \supset J \xrightarrow{4.10} P \mid I$ or $P \mid J$. □

4.6 The norm of an ideal

Still let $K = \mathbb{Q}(\sqrt{D})$ for a square-free $D \neq 0, 1$.

Definition. Let I be an ideal in $\mathcal{O}_K$. The *norm of the ideal I* is the integer $NI \geq 0$ such that $II' = (NI)$.

This integer exists by Proposition 4.11 (and it is unique, since $(n) = (m)$ for $n, m \geq 0$ implies $n = m$), so the definition makes sense.

Observation.

- $N(0) = 0$
- $I = \mathcal{O}_K \Leftrightarrow NI = 1$
Proof. “ $\Leftarrow$ ” $(1) = II' \subset I\mathcal{O}_K = I \Rightarrow I = \mathcal{O}_K$.
- $N(IJ) = NI \cdot NJ$
- $I \mid J \Rightarrow NI \mid NJ$
- If $I \mid J$ and $J \neq 0, J \neq I$, then $NI < NJ$.
- If $I = (\alpha)$ is principal, then $NI = |N\alpha|$.
Proof. $(NI) = II' = (\alpha)(\alpha') = (\alpha\alpha') = (N\alpha)$

Example. Let $K = \mathbb{Q}(\sqrt{-14})$.

For $I = (3, 1 + \sqrt{-14})$ we have

$$NI = \gcd(N3, \text{Tr}(3 \cdot (1 - \sqrt{-14})), N(1 + \sqrt{-14})) = \gcd(9, 6, 15) = 3.$$

For $J = (1 + \sqrt{-14}, 1 - \sqrt{-14})$ we have

$$NJ = \gcd(15, \text{Tr}((1 + \sqrt{-14})^2), 15) = \gcd(15, -26) = 1.$$

Hence $J = \mathcal{O}_K$.

Lemma 4.15. *If $I < \mathcal{O}_K$ is a nonzero ideal, then the factor ring $\mathcal{O}_K/I$ is finite.*

Proof. Let $n = NI$. We have the surjection

$$\begin{aligned} \mathcal{O}_K/(n) &= \mathcal{O}_K/II' \twoheadrightarrow \mathcal{O}_K/I \\ \alpha + II' &\mapsto \alpha + I \end{aligned}$$

This map is well defined, because $II' \subset I$.

So it suffices to prove that $\mathcal{O}_K/(n)$ is finite.

Consider it as an additive group. $\mathcal{O}_K(+) \simeq \mathbb{Z}^2(+)$ by Theorem 4.3. Then (n) corresponds to $(n\mathbb{Z})^2$, and hence we have isomorphisms of additive groups $\mathcal{O}_K/(n) \simeq \mathbb{Z}^2/(n\mathbb{Z})^2 = (\mathbb{Z}/n\mathbb{Z})^2$, which has n^2 elements. □

Let us note that the factor ring $\mathcal{O}_K/I$ in fact has exactly NI elements (which in a general number field serves as the definition of the norm of an ideal).

4.7 Prime ideals and factorization

Let $K = \mathbb{Q}(\sqrt{D})$, $D \neq 0, 1$ square-free.

Proposition 4.16. *Let $P < \mathcal{O}_K$ be an ideal. The following statements are equivalent:*

- a) P is a nonzero prime ideal,
- b) P is a maximal ideal,
- c) P is a proper ideal and the following holds: If $P = IJ$ for some ideals $I, J < \mathcal{O}_K$, then $I = \mathcal{O}_K$ or $J = \mathcal{O}_K$.

Proof. b) $\Rightarrow$ a) is clear.

c) $\Rightarrow$ b): Let $P \subset I$. To prove maximality we want to prove that $I = P$ or $I = \mathcal{O}_K$.

Theorem 4.10 implies $I \mid P$, i.e. $P = IJ$ for some J . By c) we then have $I = \mathcal{O}_K$ or $J = \mathcal{O}_K$. If $J = \mathcal{O}_K$, then $P = IJ = I$.

a) $\Rightarrow$ c): Let $P = IJ$. Then $P \supset IJ$, and hence $P \supset I$ or $P \supset J$ by the definition of a prime ideal; WLOG $P \supset I$. By Theorem 4.10 we then have $P \mid I$.

At the same time $I \mid P$, because $P = IJ$. Altogether we thus have $P = I$ (both inclusions hold by Theorem 4.10), and hence $P\mathcal{O}_K = P = PJ$, which by Proposition 4.13 implies $J = \mathcal{O}_K$.

This proves the proposition, but for interest let us show one more implication.

a) $\Rightarrow$ b): P a prime ideal implies that $\mathcal{O}_K/P$ is a domain. We want $\mathcal{O}_K/P$ to be a field, because then P is a maximal ideal. By Lemma 4.15 we know that $\mathcal{O}_K/P$ is finite.

Little lemma. Every finite domain is a field.

Proof. Let R be a finite domain and $\alpha \in R$, $\alpha \neq 0$.

Consider the principal ideal $(\alpha) = \{\alpha r \mid r \in R\} \subset R$.

We have $\alpha r = \alpha r' \Leftrightarrow r = r'$, because R is a domain ($\alpha(r - r') = 0 \Rightarrow r - r' = 0$).

Hence $\#(\alpha) = \#R$. But since $(\alpha) \subset R$, we have $(\alpha) = R \ni 1$, and hence $\exists \beta : \alpha\beta = 1$, i.e. α is invertible. $\square$

Remark. We have proved that $\mathcal{O}_K$ (for $K = \mathbb{Q}(\sqrt{D})$) is a *Dedekind domain*, where a domain R is Dedekind if:

- R is Noetherian.
- R is integrally closed: Let T be the field of fractions of R . R is *integrally closed* if for all $\alpha \in T$: α is integral over $R \Rightarrow \alpha \in R$.
- Every nonzero prime ideal is maximal.

Remark. The ring of integral elements $\mathcal{O}_K$ of an arbitrary number field K is Dedekind.

Unique factorization into prime ideals holds in a general Dedekind domain as well.

Theorem 4.17. *Let $K = \mathbb{Q}(\sqrt{D})$, $D \neq 0, 1$ be square-free. Every nonzero ideal $I < \mathcal{O}_K$ can be factored into a product of prime ideals*

$$I = P_1^{k_1} \cdots P_r^{k_r}, r \geq 0, k_1, \dots, k_r \in \mathbb{N},$$

where $P_1, \dots, P_r$ are pairwise distinct prime ideals. This factorization is unique up to order.

Proof.

Existence. By induction on $N(I)$:

- $N(I) = 1$. Then $I = \mathcal{O}_K$ and we choose $r = 0$.
- $N(I) > 1$. We distinguish two cases:

– I is a prime ideal. Then we have the factorization $I = I^1$.

- I is not a prime ideal; then by Proposition 4.16 we have $I = HJ$ for some ideals $H \neq \mathcal{O}_K, J \neq \mathcal{O}_K$.

The norm is multiplicative, so we have $NH, NJ < NI$, and hence H, J have a factorization by the induction hypothesis.

(Let us note that although we did the proof by induction on the norm $NI \in \mathbb{N}$, typically there are no ideals of all possible norms.)

Uniqueness. Let $P_1^{k_1} \cdots P_r^{k_r} = Q_1^{\ell_1} \cdots Q_s^{\ell_s}$.

Then $P_1 \mid Q_1^{\ell_1} \cdots Q_s^{\ell_s}$, and hence by Corollary 4.14, $P_1 \mid Q_j$ for some j . By Theorem 4.10 we then have $P_1 \supset Q_j$. But by Proposition 4.16, P_1, Q_j are maximal, so $P_1 = Q_j$.

By Proposition 4.13 we then get $P_1^{k_1-1} \cdots P_r^{k_r} = Q_1^{\ell_1} \cdots Q_j^{\ell_j-1} \cdots Q_s^{\ell_s}$ and we can continue by induction. $\square$

In Proposition 1.8 we proved that PID implies Gaussianity, so for a PID we have unique factorizations into products of elements, which are stronger than factorizations into products of prime ideals. In general there exist Gaussian domains which are not PIDs, but not in the case of $\mathcal{O}_K$:

Theorem 4.18. $\mathcal{O}_K$ is a PID if and only if it is Gaussian.

Proof. “ $\Rightarrow$ ”: Proposition 1.8

“ $\Leftarrow$ ”: We gradually prove:

(1) If π is a prime factor in $\mathcal{O}_K$, then (π) is a prime ideal.

By Lemma 1.6 it suffices to prove that $\alpha\beta \in (\pi)$ implies $\alpha \in (\pi)$ or $\beta \in (\pi)$.

Let $\alpha\beta \in (\pi)$. Then $\pi \mid \alpha\beta$, and since π is a prime factor, we have $\pi \mid \alpha$ or $\pi \mid \beta$. But this means that $\alpha \in (\pi)$ or $\beta \in (\pi)$.

(2) Every prime ideal $P < \mathcal{O}_K$ is principal.

$P = (0)$ is clearly principal; let $P \neq (0)$.

Then P divides (n) for some $n \in \mathbb{Z}$ (for example we can take $n = NP$). Consider the factorization of the number n into prime factors in $\mathcal{O}_K$: $n \parallel \pi_1^{k_1} \cdots \pi_r^{k_r}$.

We have $P \mid (n) = (\pi_1)^{k_1} \cdots (\pi_r)^{k_r}$, and hence $P \mid (\pi_j)$ for some j (Corollary 4.14), because P is a prime ideal.

By (1) we have that (π_j) is a nonzero prime ideal, hence a maximal ideal by Proposition 4.16. Moreover $P \supset (\pi_j)$ by Theorem 4.10, and hence $P = (\pi_j)$ is a principal ideal.

(3) Every ideal is principal.

$$I \stackrel{4.17}{=} P_1^{k_1} \cdots P_r^{k_r} \stackrel{(2)}{=} (\pi_1)^{k_1} \cdots (\pi_r)^{k_r} = (\pi_1^{k_1} \cdots \pi_r^{k_r}).$$

$\square$

4.8 Description of prime ideals

Let $K = \mathbb{Q}(\sqrt{D})$, $D \neq 0, 1$ be square-free. We want to describe explicitly what the prime ideals in $\mathcal{O}_K$ look like. For example, we know that:

Example. In $\mathbb{Z}[i]$ every ideal is principal and there are three types of prime ideals, which we get by factoring the primes $p \in \mathbb{N}$:

- $(2) = (1+i)^2$, where $(1+i)$ is a prime ideal,
- for a prime $p \equiv 3 \pmod{4}$, (p) is a prime ideal,
- for a prime $p \equiv 1 \pmod{4}$ there is a unique (up to order) expression $p = a^2 + b^2$ with $a, b \in \mathbb{N}$ and the corresponding factorization $(p) = (a+bi)(a-bi)$, where $(a+bi), (a-bi)$ are distinct prime ideals.

For example $(5) = (2+i)(2-i)$, $(13) = (3+2i)(3-2i)$.

Similar three possibilities occur in general, as we prove shortly.

Lemma 4.19. *Let P be a nonzero prime ideal in $\mathcal{O}_K$. Then*

- a) $\exists!$ prime $p \in \mathbb{N} : P \mid (p)$.
- b) $N(P) = p$ or p^2 .
- c) If I is an ideal in $\mathcal{O}_K$ such that $N(I) = p$ is a prime, then I is a prime ideal.

Proof.

a) Let $n = N(P)$ and consider the prime factorization $n = p_1^{k_1} \cdots p_r^{k_r}$ in $\mathbb{Z}$.

Then $P \mid PP' = (N(P)) = (p_1)^{k_1} \cdots (p_r)^{k_r}$, and hence $P \mid (p_j)$ for some j . It remains to prove uniqueness.

Let $P \mid (p), (q)$, where $p \neq q$ are primes in $\mathbb{Z}$. By Bézout's identity there are $a, b \in \mathbb{Z}$ such that $ap + bq = 1$. But then $P \mid (ap + bq) = (1) = \mathcal{O}_K$, which contradicts the fact that P is a prime ideal.

b) $P \mid (p) \Rightarrow N(P) \mid N((p)) = p^2$. Hence $N(P)$ can be $1, p$ or p^2 , but $N(P) = 1$ is not possible, because $P \neq \mathcal{O}_K$.

c) Let I not be a prime ideal, i.e. by Proposition 4.16 we have $I = AB$ for proper ideals A, B . But then $p = NI = NA \cdot NB$, and hence NA or NB equals 1, which implies $A = \mathcal{O}_K$ or $B = \mathcal{O}_K$. $\square$

Theorem 4.20. *Let $\mathcal{O}_K = \mathbb{Z}[\omega]$, where*

$$\omega = \begin{cases} \sqrt{D} \\ \frac{1+\sqrt{D}}{2} \end{cases} \quad \text{has the minimal polynomial } f(x) = \begin{cases} x^2 - D & \text{for } D \equiv 2, 3 \pmod{4} \\ x^2 - x + \frac{1-D}{4} & \text{for } D \equiv 1 \pmod{4} \end{cases}$$

If $p \in \mathbb{Z}$ is a prime, then the factorization of (p) into prime ideals in $\mathcal{O}_K$ corresponds to the factorization of the polynomial $(f(x) \bmod p) \in \mathbb{F}_p[x]$ into a product of irreducible polynomials.

Three cases can occur:

- a) $f(x) \bmod p$ is irreducible. Then (p) is a prime ideal with norm p^2 .
- b) $f(x) \equiv (x - c)(x - d) \bmod p$ for some $c \not\equiv d \bmod p$. Then $(p) = PP'$ for prime ideals $P \neq P'$, $N(P) = N(P') = p$.
- c) $f(x) \equiv (x - c)^2 \bmod p$ for some c . Then $(p) = P^2$ for a prime ideal P such that $N(P) = p$.

Proof. We have

$$\begin{aligned} \mathcal{O}_K &= \mathbb{Z}[\omega] \simeq \mathbb{Z}[x]/(f(x)) \\ a + b\omega &\mapsto a + bx \end{aligned}$$

and

$$\begin{aligned} \mathcal{O}_K/(p) &\simeq \mathbb{Z}[x]/(p, f(x)) \simeq \mathbb{F}_p[x]/(f(x)) \\ (a + b\omega) \bmod p &\longmapsto (a \bmod p) + (b \bmod p)x \end{aligned}$$

Let us distinguish what $\mathbb{F}_p[x]/(f(x))$ looks like in our three cases:

- a) $f(x) \bmod p$ is irreducible. Then $\mathbb{F}_p[x]/(f(x))$ is a field.
- b) $f(x) \equiv (x - c)(x - d) \bmod p$ for $c \not\equiv d \bmod p$. By the Chinese remainder theorem we then have

$$\mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_p[x]/(x - c) \times \mathbb{F}_p[x]/(x - d) \simeq \mathbb{F}_p \times \mathbb{F}_p.$$

So it is not a field and it contains no *nilpotent*, which is an element $u \neq 0$ such that $u^k = 0$ for some k .

- c) $f(x) \equiv (x - c)^2 \bmod p$. Then $\mathbb{F}_p[x]/(x - c)^2$ is not a field and contains the nilpotent $(x - c)$, because $(x - c)^2 \equiv 0 \bmod (x - c)^2$.

Similarly, let us consider what $\mathcal{O}_K/(p)$ looks like. Thanks to the isomorphism $\mathcal{O}_K/(p) \simeq \mathbb{F}_p[x]/(f(x))$ it must correspond to the cases above:

a) $\mathcal{O}_K/(p)$ is a field. Then (p) is a maximal ideal, and hence by Proposition 4.16, (p) is a prime ideal.

b,c) $\mathcal{O}_K/(p)$ is not a field, and hence (p) is not a prime ideal.

Then $(p) = PI$ for proper ideals $P, I < \mathcal{O}_K$. We have $N(p) = p^2 = N(P) \cdot N(I)$, and hence $N(P) = N(I) = p$. By Lemma 4.19c), P, I are then prime ideals.

At the same time, by the definition of the norm we have $(p) = (N(P)) = PP'$, hence $P' = I$ thanks to the unique factorization 4.17.

It remains to distinguish two cases:

- If $P = P'$, then $\mathcal{O}_K/(p) = \mathcal{O}_K/P^2$ contains a nonzero nilpotent, namely the image of any element $\alpha \in P \setminus P^2$ (indeed, $\alpha \notin P^2$ and $\alpha^2 \in P^2$). So this is case c).
- If $P \neq P'$, then $\mathcal{O}_K/(p) = \mathcal{O}_K/PP' \stackrel{\text{CRT}}{\simeq} \mathcal{O}_K/P \times \mathcal{O}_K/P'$, where $\mathcal{O}_K/P, \mathcal{O}_K/P'$ are fields, because P, P' are (distinct, hence comaximal) maximal ideals. Hence $\mathcal{O}_K/(p)$ contains no nilpotents. So this is case b).

The verification of the norms is trivial. □

In this way we can also determine explicitly what the factorization into prime ideals looks like:

Theorem 4.21. *Let $p \in \mathbb{N}$ be a prime such that (p) is not a prime ideal in $\mathcal{O}_K$. Then $f(x) \equiv (x - c)(x - d) \pmod{p}$ (where possibly $c \equiv d \pmod{p}$) and we have $(p) = (p, \omega - c)(p, \omega - d)$.*

Proof. By Theorem 4.20 we have $(p) = PP'$ and $f(x) \equiv (x - c)(x - d) \pmod{p}$.

Let $I = (p, \omega - c)$. Then $I = (p, \omega - c) \supset (p)$, and hence $I \mid (p) = PP'$. We have $\omega - c \notin (p)$ (exercise), and hence $I \neq (p)$. So $I = P$ or $I = P'$ or $I = \mathcal{O}_K$; we want to prove that $I \neq \mathcal{O}_K$, i.e. that $N(I) \neq 1$. By Proposition 4.11 we have $N(I) = \gcd(N(p), \text{Tr}(p(\omega - c)), N(\omega - c))$. Let us compute these values:

- $N(p) = p^2$
- $\text{Tr}(p(\omega - c)) = p \text{Tr}(\omega - c)$
- $N(\omega - c) = (\omega - c)(\omega - c)' = (c - \omega)(c - \omega') = f(c) \equiv 0 \pmod{p}$.

It follows that all these numbers are divisible by p , and hence $p \mid N(I) \neq 1$. Therefore $I \neq \mathcal{O}_K$, and hence $I = P$ or P' is a prime ideal.

Similarly we have that $(p, \omega - d) = P$ or P' is a prime ideal.

At the same time we have $P = P' \Leftrightarrow c \equiv d \pmod{p} \Leftrightarrow (p, \omega - c) = (p, \omega - d)$. In each case we get $(p) = PP' = (p, \omega - c)(p, \omega - d)$. □

Theorems 4.20 and 4.21 allow us to find the factorization of an arbitrary ideal I in $\mathcal{O}_K$ into prime ideals, for example as follows:

1. Factor $N(I)$ into a product of primes $N(I) = p_1^{k_1} \cdots p_r^{k_r}$ in $\mathbb{Z}$.
2. Factor every (p_i) into a product of prime ideals in $\mathcal{O}_K$.
3. This gives the factorization of the ideal $(N(I)) = P_1^{\ell_1} \cdots P_s^{\ell_s}$ into a product of prime ideals in $\mathcal{O}_K$.
4. At the same time we have $I \mid II' = (N(I))$, and hence $I = P_1^{m_1} \cdots P_s^{m_s}$ for some $0 \leq m_i \leq \ell_i$.
5. Find the correct values of m_i : at worst one can try all possible combinations, but considering the norms of ideals helps a lot; basically it is about choosing correctly between P_i and P'_i every time.

4.9 Examples in $K = \mathbb{Q}(\sqrt{-14})$

In this section let $K = \mathbb{Q}(\sqrt{-14})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$.

Example. How to find prime ideals?

- We are interested in $x^2 + 14 \pmod{p}$, i.e. $x^2 \equiv -14 \pmod{p}$
- $f(x) \pmod{p}$ reducible $\Leftrightarrow -14$ is a quadratic residue modulo p (for $p \nmid 14$).
- $p = 2, x^2 \equiv -14 \pmod{2} \Rightarrow x \equiv 0 \pmod{2}$ (0 is a double root)
 $(2) = P_2^2$ for $P_2 = (2, \sqrt{-14})$
- $p = 3, x^2 \equiv -14 \equiv 1 \pmod{3} \Rightarrow x = \pm 1$
 $(3) = P_3 \cdot P_3'$ for $P_3 = (3, \sqrt{-14} + 1)$
- $p = 5, x^2 \equiv -14 \equiv 1 \pmod{5} \Rightarrow x = \pm 1$
 $(5) = P_5 \cdot P_5'$ for $P_5 = (5, \sqrt{-14} + 1)$
- $p = 7, (7) = P_7^2$ for $P_7 = (7, \sqrt{-14})$
- $p = 11, x^2 \equiv -14 \equiv 8 \pmod{11}$, 8 is not a quadratic residue modulo 11 $\Rightarrow (11)$ is a prime ideal
- $p = 13, x^2 \equiv -14 \equiv -1 \pmod{13} \Rightarrow x = \pm 5$
 $(13) = P_{13} \cdot P_{13}'$ for $P_{13} = (13, \sqrt{-14} + 5)$

Example. Factor $(1 + \sqrt{-14})$ into a product of prime ideals

$$N(1 + \sqrt{-14}) = 1 + 14 = 15 = 3 \cdot 5$$

Does $1 + \sqrt{-14} \in P_3$ hold? Yes

Also $1 + \sqrt{-14} \in P_5$. Hence $(1 + \sqrt{-14}) = P_3 \cdot P_5$

Example. Factor $(2 + 3\sqrt{-14})$

$$N(2 + 3\sqrt{-14}) = 4 + 9 \cdot 14 = 130 = 2 \cdot 5 \cdot 13$$

$$2 + 3\sqrt{-14} \in P_2$$

$$2 + 3\sqrt{-14} \in P_5? \quad 2 + 3\sqrt{-14} - 3(\sqrt{-14} + 1) = -1 \notin P_5 \Rightarrow 2 + 3\sqrt{-14} \notin P_5$$

$$2 + 3\sqrt{-14} - 3(\sqrt{-14} + 5) = -13 \in P_{13}, \text{ hence } 2 + 3\sqrt{-14} \in P_{13}$$

$$(2 + 3\sqrt{-14}) = P_2 \cdot P_5' \cdot P_{13}$$

Example. Factor $(5 + 2\sqrt{-14})$.

$$N(5 + 2\sqrt{-14}) = 25 + 4 \cdot 14 = 25 + 56 = 81 = 3^4.$$

If $P_3, P_3' \mid (5 + 2\sqrt{-14})$, then $(3) \mid (5 + 2\sqrt{-14})$, which would mean $3 \mid 5 + 2\sqrt{-14}$ in $\mathcal{O}_K$, but that is not true.

Hence only one of P_3, P_3' divides $(5 + 2\sqrt{-14})$

$$5 + 2\sqrt{-14} - 2(\sqrt{-14} + 1) = 3 \in P_3, \text{ hence } P_3 \mid (5 + 2\sqrt{-14}) \text{ and therefore } (5 + 2\sqrt{-14}) = P_3^4$$

Example. Factor $(1 + \sqrt{-14}, 5 + 2\sqrt{-14})$

$$(1 + \sqrt{-14}) = P_3 \cdot P_5, (5 + 2\sqrt{-14}) = P_3^4$$

$$\text{Hence } (1 + \sqrt{-14}, 5 + 2\sqrt{-14}) = P_3$$

5. Exercise sheets

In the version from the winter semester 2023/2024 by Matěj Doležálek. (Partial) solutions follow in the next chapter.

5.1 Exercises 1

ideals, operations on ideals, prime ideals, maximal ideals

1. Prove that the union of a chain of (arbitrarily many) ideals $I_1 \subset I_2 \subset I_3 \subset \dots$ is an ideal.
2. For ideals I, J define $I + J := \{a + b \mid a \in I, b \in J\}$. Prove that $I + J$ is the smallest ideal in R which contains I and J .
3. Let R be a ring and M an ideal in R . Prove:
 - a) M is maximal if and only if $R = M + aR$ for all $a \in R \setminus M$.
 - b) If M is maximal and $a \in R \setminus M$, then there are $m \in M$ and $r \in R$ such that $1 = m + ar$.
4. Let us have ideals I, J, K of a ring R . Prove that $IJ \subset I \cap J$ and $I(J + K) = IJ + IK$. Find an example where $IJ \neq I \cap J$.
5. Determine: $\mathbb{Q}[x]/(x + 2)$, $\mathbb{Q}[x]/(x^2 - 2)$, $\mathbb{Q}[x]/(x^2 - 1)$, $\mathbb{R}[x]/(x^2 - 2)$, $\mathbb{Z}[x]/(x^2 - 2)$.
6. Prove that the operations on a factor ring are well defined and that it is a ring (and prove the other things from the lecture that we left as exercises).
7. Prove the 3rd isomorphism theorem: If R is a ring, $I < R$ an ideal and $S \subset R$ a subring, then $S + I$ is a subring in R and $(S + I)/I \simeq S/(S \cap I)$.
8. Consider the ring $\mathbb{Z}$ and the ideals $I = (168)$ and $J = (288)$ in it.
 - a) What do all maximal ideals and prime ideals in $\mathbb{Z}$ look like?
 - b) Determine $I + J, IJ, I \cap J, I^2 + J$.
 - c) Find all prime ideals which contain the ideal $I, J, IJ, I \cap J$, resp. J^2 .
9. Let R be a principal ideal domain and $a, b \in R$.
 - a) Determine $(a)(b), (a) + (b), (a) \cap (b)$.
 - b) What do all maximal ideals and prime ideals in R look like?
 - c) Prove that the factor of R by a nonzero prime ideal is a field.
10. For subsets A, B of a ring R define $A \odot B := \{ab \mid a \in A, b \in B\}$ (beware, this does not correspond to the multiplication of ideals). Let I be an ideal in R . Prove that $(a + I) \odot (b + I) \subset ab + I$. Does the opposite inclusion hold?
11. Consider the principal ideal domain $\mathbb{Q}[x]$ and the ideals $I = (x^3 + x^2 + 2x + 2)$ and $J = (x^3 - 2x^2 + 2x - 4)$.
 - a) Determine $I + J, IJ, I \cap J, I^2 + J^3$.
 - b) Which factors modulo the principal ideals from part a) are domains?
 - c) Find all prime ideals which contain the ideal $I, J, IJ, I \cap J$, resp. J^2 .

12. Let R be a Noetherian ring and $I < R$ an ideal. Prove that R/I is Noetherian as well.
13. We are given a ring R in which for every $x \in R$ there is an integer $n \geq 2$ such that $x^n = x$. Prove that every prime ideal in R is maximal.

Hints

5. 1st isomorphism theorem + sometimes the Chinese remainder theorem.
7. The projection $\pi: R \twoheadrightarrow R/I$ and its restriction to $\varphi: S \rightarrow R/I$. The 1st isomorphism theorem for φ .
10. It does not. Choose $R = \mathbb{Z}$ and a prime in $ab + I$.
12. The ideals in R/I are exactly of the form J/I for $J < R$, $J \supset I$.
13. Find the inverse in the factor ring.

5.2 Exercises 2

Gauss's lemma, the Chinese remainder theorem, applications of Zorn's lemma

- Let R be a Gaussian domain and T its field of fractions. For every irreducible polynomial $f \in T[x]$ there is $u \in T \setminus \{0\}$ such that uf is an irreducible element of $R[x]$.
- Let K be a field. Then $K[x, y]$ and $K[x_1, x_2, \dots]$ (infinitely many variables) are Gaussian, but $K[x, y]$ is not a principal ideal domain (though it is Noetherian) and $K[x_1, x_2, \dots]$ is neither Noetherian nor a principal ideal domain.
- Describe all ideals in the ring $\mathbb{Z}/(150)$ and characterize which pairs of them are comaximal.
- Let R be a ring. Using Zorn's lemma, prove that every proper ideal is contained in some maximal ideal.
- Use the proof of the Chinese remainder theorem (in particular the step where $1 = a_1 + a_2$) to construct an explicit isomorphism $\mathbb{Z}/(n) \times \mathbb{Z}/(m) \simeq \mathbb{Z}/(mn)$ for $n = 16, m = 35$. Which well-known theorem does the step in parentheses correspond to?
- Realize that in an ordered set $\mathcal{A}$ there can also exist an uncountable chain $\mathcal{B}$ for whose indexing the natural numbers are not enough. Find a couple of examples of such a situation. (There is no catch in it; it is just so that one does not get the impression that in Zorn's lemma it suffices to deal with chains indexed by natural numbers.)
- Show that if $\varphi: R \rightarrow S$ is a ring homomorphism, then the relations $\psi(r) := \varphi(r)$ for $r \in R$ and $\psi(x) := x$ are satisfied by exactly one homomorphism $\psi: R[x] \rightarrow S[x]$. Moreover, ψ is injective/surjective if and only if φ is injective/surjective.
- Let R be a ring and $I_1, \dots, I_n$ pairwise comaximal ideals in R . Realize that from the CRT we have in particular an isomorphism of multiplicative groups $(R/(I_1 \cdots I_n))^\times \simeq (R/I_1)^\times \times \cdots \times (R/I_n)^\times$. As an application of this fact, think about why for odd primes $p \neq q$ the group $(\mathbb{Z}/(pq))^\times$ cannot be cyclic.
- Prove using Zorn's lemma: in a vector space, any linearly independent set can be extended to a basis.
- Let $(M, \leq)$ be a partially ordered set. Prove using Zorn's lemma that the ordering $\leq$ can be extended to a linear ordering, i.e. that there is an ordering $\preceq$ on M which is linear and satisfies: $x \leq y \Rightarrow x \preceq y$ for all $x, y \in M$.
- Let R be a Gaussian domain and T its field of fractions. Let us have a non-constant primitive polynomial $f \in R[x]$. Then f is irreducible in $T[x]$ if and only if it is irreducible in $R[x]$.
- * Let F be a finite field. Show that any map $g: F \rightarrow F$ can be written as a polynomial.

- 13.** * (Eisenstein's criterion) Let us have a primitive polynomial $f = a_n x^n + \cdots + a_1 x + a_0$ with integer coefficients and a prime p . Prove that if $p \nmid a_n$, $p \mid a_i$ for $i = 0, 1, \dots, n-1$ and $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Z}$. Try to think about a generalization for a general integral domain R instead of $\mathbb{Z}$.
- 14.** * Using Zorn's lemma, prove that if a ring R has a proper ideal which is not finitely generated, then it also has a prime ideal which is not finitely generated.

Hints

- 12.** The Chinese remainder theorem in $F[x]$. Linear polynomials give maximal ideals. (Alternatively Lagrange interpolation.)
- 13.** Assume for a contradiction that $f = gh$, map the whole situation by the projection $\mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ and use unique factorizations.

5.3 Exercises 3

root fields and splitting fields, algebraic closure, the Galois group, separability

- Let α be an algebraic element over a field T . Then $[T(\alpha) : T] = \deg m_{\alpha, T}$.
- For a field T and a polynomial $f(x)$ determine all possible root fields for f over T , the splitting field for f over T , the degrees of all these field extensions and also their Galois groups over T :
 - $f(x) = x^2 + 3$, $T = \mathbb{R}$,
 - $f(x) = x^2 - 1$, $T = \mathbb{Q}$,
 - *c) $f(x) = x^3 - 2$, $T = \mathbb{Q}$.
- Let us have fields $T \subset U \subset V$. If V is algebraic over U and U is algebraic over T , then V is also algebraic over T .
- Let $U \supset T$ be a field extension and $\alpha \in U$ a root of *some* separable $f \in T[x]$. Then α is separable over T .
- A field extension of finite degree is necessarily algebraic.
- Let us have field extensions $V \supset U \supset T$. Then $[V : T] = [V : U] \cdot [U : T]$.
- Let $T \subset U$ be an algebraic field extension and $U \subset K$ (not necessarily algebraic). Then K is an algebraic closure of U if and only if K is an algebraic closure of T .
- Let $\varphi : K \rightarrow R$ be a ring homomorphism. Recall that when K is a field, φ must be injective.
- For a field T and a polynomial $f(x)$ determine all possible root fields for f over T , the splitting field for f over T , the degrees of all these field extensions and (possibly) also their Galois groups over T :
 - $f(x) = x^2 + 1$, $T = \mathbb{Q}$,
 - b) $f(x) = x^4 - 1$, $T = \mathbb{Q}$,
 - *c) $f(x) = x^2 + 1$, $T = \mathbb{Z}_7$,
 - **d) $f(x) = x^n - 1$, $T = \mathbb{Q}$, $n \in \mathbb{N}$.
- Let $S \supset T$ be fields, S algebraically closed and $U = \{\alpha \in S \mid \alpha \text{ algebraic over } T\}$. Then U is an algebraic closure of T . (Proposition 2.8 of the notes)
- Let T, U be fields of characteristic 0. Then $\mathbb{Q} \subset T, U$ and every homomorphism $\varphi : T \rightarrow U$ is a $\mathbb{Q}$ -homomorphism. (In characteristic p the field $\mathbb{Z}_p$ has the same property.)
- An element α is algebraic over a field T if and only if $T(\alpha) = T[\alpha]$.
- * No finite field is algebraically closed.
- * Let p be a prime, $T = \mathbb{Z}_p(y)$ and $U = T(\sqrt[p]{y})$. Determine $[U : T]$, $[U : T]_s$ and $\text{Gal}(U/T)$.
- * The algebraic closure of an infinite field T has the same cardinality as T .

Hints

4. $m_{\alpha, T} \mid f$.
11. A homomorphism must leave in place the whole subfield generated by the one (the so-called *prime field*).
12. From the minimal polynomial you produce the inverse (and vice versa).
13. Start with a polynomial whose roots are all the elements.
14. $x^p - y \in \mathbb{Z}_p[y][x]$ is irreducible by Eisenstein, but it has only one p -fold root.
15. Think about why $\#T[x] = \#T$, so that when we add (in one step) the roots of all polynomials, the cardinality is preserved.

5.4 Exercises 4

separable, normal, simple and Galois extensions

1. Let $U \supset T$ be an extension of finite degree. Prove that it is Galois if and only if $[U : T] = \# \text{Gal}(U/T)$.
2. (preservation and composition of distinguished properties) Let $V \supset U \supset T$ be field extensions. If you know that the extension $V \supset T$ has property X , decide whether $V \supset U$ or $U \supset T$ must necessarily have property X as well. If you know that both $V \supset U$, $U \supset T$ have property X , decide whether $V \supset T$ must necessarily have it as well.
 - a) $X =$ of finite degree,
 - b) $X =$ algebraic,
 - c) $X =$ separable,
 - d) $X =$ normal,
 - e) $X =$ Galois.
3. Decide for the following extensions which of the distinguished properties from Problem 2. they have and which they do not:
 - a) $\mathbb{C} \supset \mathbb{R}$,
 - b) $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$,
 - *c) $\mathbb{Z}_p(x) \supset \mathbb{Z}_p$,
 - *d) $\overline{\mathbb{Q}} \supset \mathbb{Q}$.
4. Let $V \supset T$ be a Galois extension and $V \supset U \supset T$. Prove that $[U : T] = \frac{\# \text{Gal}(V/T)}{\# \text{Gal}(V/U)}$.
5. Let $f \in T[x]$ be a polynomial with the factorization into mutually non-associated irreducible polynomials $f = f_1 \cdots f_k$. Consider the Galois group of the splitting field of f over T as a group of permutations of the set of roots of f . Show that each of these permutations must have at least k cycles.
6. (review from the lecture) Let U be a field, $G < \text{Aut}(U)$ a subgroup and $T \subset U$ a subfield. Then $\text{Gal}(U/\text{Fix}(U, G)) \supset G$ and $\text{Fix}(U, \text{Gal}(U/T)) \supset T$.
7. Let $U \supset T$ be a separable extension of finite degree. Show that there is a field V such that $U \subset V$, $[V : T] \leq ([U : T])!$ and the extension $V \supset T$ is Galois.
8. By Proposition 2.26, if $U \supset T$ is an algebraic extension, then every T -homomorphism $\varphi : U \rightarrow U$ must even be a T -automorphism. Think about why algebraicity is necessary – for $T = \mathbb{Z}_p$, $U = T(x)$ (the field of rational functions) find a T -homomorphism $\varphi : U \rightarrow U$ which is not a T -automorphism.
9. Let T be a field with $\text{char } T \neq 2$ and $a, b \in T$ elements with $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin T$. Then $[T(\sqrt{a}, \sqrt{b}) : T] = 4$.

* You can try to prove $\text{Gal}(T(\sqrt{a}, \sqrt{b})/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
10. An extension $U \supset T$ is normal if and only if there exists a set $\mathcal{M} \subset T[x]$ such that U is a splitting field of the set $\mathcal{M}$ over T .
11. * (existence of the separable closure) Let $U \supset T$ be a field extension. All the elements $\alpha \in U$ that are separable over T form a subfield of U .

12. * Let p be a prime, $U = \mathbb{Z}_p(x, y)$, $T = \mathbb{Z}_p(x^p, y^p)$. Prove that the extension $U \supset T$ is not simple.

Hints

4. It suffices to combine **2.e)** and **1.**.
7. You have a simple extension; factor the minimal polynomial.
11. Realise that any two separable elements generate a separable extension.
12. If $U = T(r)$, observe that $r^p \in T$ and derive a contradiction using degrees.

5.5 Exercises 5

computing Galois groups, the Galois correspondence

In this exercise sheet, to *determine* a Galois group means for us to find some “known” group it is isomorphic to, and to figure out how the individual automorphisms act. Known groups are for instance $\mathbb{Z}_n$, D_{2n} , S_n , or products of known groups.

1. Determine the Galois group of $T \supset \mathbb{Q}$ and all fields U , $T \supset U \supset \mathbb{Q}$, if

- a) $T = \mathbb{Q}(i, \sqrt{2})$,
- b) $T =$ the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

2. For the field extension $U \supset T$ determine $[U : T]$ together with a basis of U as a vector space over T , decide whether it is a Galois extension, and if so, determine also all the fields V , $U \supset V \supset T$, if

- a) $U = \mathbb{Q}(\sqrt{2}, e^{2\pi i/3})$, $T = \mathbb{Q}$,
- b) $U = \mathbb{Q}(\sqrt[3]{3})$, $T = \mathbb{Q}$,
- c) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $T = \mathbb{Q}$,
- d) $U = \mathbb{Q}(\sqrt{1 + \sqrt{2}})$, $T = \mathbb{Q}$.

3. Let U be the splitting field of a polynomial f over a field T . Determine U , $[U : T]$, a basis of U over T and $\text{Gal}(U/T)$ (you may also think about the fields V , $U \supset V \supset T$, but they often look rather ugly), if

- a) $f = x^2 - 5$, $T = \mathbb{Q}$,
- b) $f = x^3 - 2$, $T = \mathbb{Q}(e^{2\pi i/3})$,
- c) $f = (x^2 - 3)(x^2 - 5)$, $T = \mathbb{Q}(\sqrt{2})$,
- *d) $f = (x^2 - 1)^2 - 2$, $T = \mathbb{Q}$.

4. Let us have fields $V \supset U \supset T$ such that both $V \supset T$ and $U \supset T$ are normal extensions. Then $\text{Gal}(V/U) \triangleleft \text{Gal}(V/T)$ and $\text{Gal}(V/T)/\text{Gal}(V/U) \simeq \text{Gal}(U/T)$.

5. Let us consider cyclotomic fields.

- a) Recall that $\text{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$. Assume that you already know $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$.
- b) Let U be the splitting field of $x^{20} - 1$ over $\mathbb{Q}(i)$. Determine $\text{Gal}(U/\mathbb{Q}(i))$ and all the intermediate fields V , $U \supset V \supset \mathbb{Q}(i)$.
- c) * Let U be a root field of $x^3 + x^2 - 2x - 1$ over $\mathbb{Q}$. Determine $\text{Gal}(U/\mathbb{Q})$.

6. Let us have an extension $U \supset \mathbb{Q}$ of finite degree which, however, is not normal. Think about whether we can nevertheless *somehow* use the Galois correspondence to find all the fields V , $U \supset V \supset \mathbb{Q}$. More generally, consider the same for an extension $U \supset T$ which is separable and of finite degree, but is not normal.

7. * Let U be the splitting field of a polynomial f over a field T . Determine U , $[U : T]$, a basis of U over T and $\text{Gal}(U/T)$ and all the fields V , $U \supset V \supset T$, if

- a) $f = x^3 - 5$, $T = \mathbb{Z}_7$,
- b) $f = x^4 - 3$, $T = \mathbb{Z}_5$,
- c) $f = x^{p^k} - x$, $T = \mathbb{Z}_p$.

8. ** Observe that if $\text{Gal}(T/\mathbb{Q}) \simeq A_4$, then there is no field U , $T \supset U \supset \mathbb{Q}$, with degree $[U : \mathbb{Q}] = 2$. If you feel confident, try to prove that the splitting field of $f = x^4 + 8x + 12$ over $\mathbb{Q}$ is an example

of such a T . (I have not managed to prove it so far, but according to a trustworthy source it should be true.)

Hints

5. b) Look at $\text{Gal}(U/\mathbb{Q}(i))$ inside $\text{Gal}(U/\mathbb{Q})$, whose structure you know. c) Look inside the seventh cyclotomic field.
6. Isn't it enough to look at everything inside a larger extension which is Galois?
7. a), b) What cube/fourth roots of unity does $\mathbb{Z}_7/\mathbb{Z}_5$ have? c) A trick: the set of roots is closed under both addition and multiplication.

5.6 Exercises 6

algebraic sets, Hilbert's Nullstellensatz, radicals

1. Decide which of the following sets are algebraic:

- | | |
|--|---|
| a) $\{(t, t^2, t^3) \in K^3 \mid t \in K\}$, | d) ${}^*\mathbb{Z}^2$ as a subset of $\mathbb{R}^2$, |
| b) $\{(\cos t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$, | e) ${}^*\{(t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$. |
| c) $\mathbb{Z}$ as a subset of $\mathbb{R}$, | |

2. (a counterexample to Hilbert's theorem without algebraic closedness) Find in $\mathbb{R}[x]$ a maximal ideal which contains no linear polynomial.

3. The *Jacobson radical* of a ring R is defined as $\mathcal{J}(R) := \bigcap_{M < R \text{ maximal}} M$. Observe that $a \in \mathcal{J}(R)$ if and only if $1 - ar$ is a unit for every $r \in R$.

4. In the domain of the integers $\mathbb{Z}$ determine

- a) $\sqrt{(0)}$, $\mathcal{J}(\mathbb{Z})$,
- b) $\sqrt{(25)}$, $\sqrt{(125)}$, $\sqrt{(50)}$, $\sqrt{(100)}$, $\sqrt{(\prod_i p_i^{r_i})}$ for pairwise distinct primes p_i .

Further determine

- c) $\mathcal{J}(\mathbb{Z}/(100))$,
- d) * when $(\mathbb{Z}/(n))/\mathcal{J}(\mathbb{Z}/(n))$ is a field.

5. In the domain $\mathbb{C}[x]$ of polynomials over the complex numbers

- a) compute $\sqrt{(0)}$, $\mathcal{J}(\mathbb{C}[x])$, $\sqrt{(x-3)^5(x-1)^4(x^3+2)}$, $\sqrt{(x^6-x^4-x^2+1)}$,
- b) prove that $\sqrt{(p)} = (\frac{p}{\gcd(p, p')})$, where $p \in \mathbb{C}[x]$.

6. Let us work over $K = \mathbb{C}$:

- a) Prove that $I(V(x^2 - y)) = (x^2 - y)$ and that the algebraic set $V(x^2 - y) \subset \mathbb{C}^2$ is irreducible.
- b) Determine the set $V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \subset \mathbb{C}^2$ and decompose it into irreducible components.
- c) * Decompose $V(x^2 + y^2 - 1, x^2 - z^2 - 1) \subset \mathbb{C}^3$ into irreducible components.

7. If K is a finite field, then every subset of K^n is algebraic.

8. Observe that for an ideal $I < R$ the radical $\sqrt{I}$ equals $\pi^{-1}(\sqrt{0/I})$, where $\pi : R \twoheadrightarrow R/I$ is the natural projection.

9. Let K be an infinite field and $V = \{(t, t^2, t^3, \dots, t^n) \mid t \in K\} \subset K^n$. Determine $I(V)$ (with a proof!) and, using the problem from the homework (V irreducible $\iff I(V)$ a prime ideal), deduce that V is irreducible.

10. Think through the following characterisations of ideals by means of factor rings: $I < R$ is

- maximal if and only if all nonzero elements of R/I are invertible,
- a prime ideal if and only if a product of nonzero elements in R/I is always nonzero,

- a radical ideal if and only if a power of a nonzero element in R/I is always nonzero.

11. Prove that $f(x, y) = y^2 + x^2(x-1)^2 \in \mathbb{R}[x, y]$ is an irreducible polynomial, but the set $V(f) \subset \mathbb{R}^2$ is reducible.

Hints

- 7. One-point sets are always algebraic.
- 9. Reduce everything to one variable.

5.7 Exercises 7

Algebraic number theory

- Find all units in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ for $D = -2, -3, -7$.
* If you have ever seen Pell's equation, try also $D = 2, 5$.
- Irreducible elements for $K = \mathbb{Q}(\sqrt{-14})$:
 - If an element $\alpha \in \mathcal{O}_K$ has norm p , which is a prime in $\mathbb{Z}$, then α is irreducible in $\mathcal{O}_K$.
 - Find some irreducible element of $\mathbb{Z}[\sqrt{-14}]$ with prime norm.
 - Prove that 3 and $1 + \sqrt{-14}$ are irreducible.
 - Prove that $3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$ are two different irreducible factorisations.
- Principal ideals for $K = \mathbb{Q}(\sqrt{-14})$:
 - Prove that $(17 + 2\sqrt{-14}, 20 + \sqrt{-14}) = (3 - \sqrt{-14})$ is a principal ideal in $\mathbb{Z}[\sqrt{-14}]$.
 - $(2, \sqrt{-14})$ is not a principal ideal in $\mathbb{Z}[\sqrt{-14}]$.
 - Prove that $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14})$ and that this is a proper ideal which is not principal.
- Multiplication of ideals for $K = \mathbb{Q}(\sqrt{-14})$:
 - $(5 + \sqrt{-14}, 2 + \sqrt{-14})(4 + \sqrt{-14}, 2 - \sqrt{-14}) = (6, 3\sqrt{-14})$.
 - Let $I = (3, 1 + \sqrt{-14})$. Then $II' = (3)$, I is not principal and $I \neq I'$.
 - Let $J = (5, 1 + \sqrt{-14})$. Then $(15) = IJJ'$. Use this to find two different irreducible factorisations of 15.
 - * I, J are prime ideals.
- Let G be a subgroup of the additive group $\mathbb{Z}^n$, where $n \in \mathbb{N}$. Prove that $G \simeq \mathbb{Z}^m$ for some m , $0 \leq m \leq n$. As a consequence, observe that an arbitrary ideal in $\mathcal{O}_K$ can be written with at most two generators.
- Let $K = \mathbb{Q}(\sqrt{D})$ and $\omega = \sqrt{D}$, resp. $\frac{1+\sqrt{D}}{2}$ for $D \equiv 2, 3$, resp. $1 \pmod{4}$. For $m \in \mathbb{Z}$ and $\alpha = a + b\omega \in \mathcal{O}_K$ prove that $m \mid \alpha$ in $\mathcal{O}_K$ if and only if $m \mid a, b$ in $\mathbb{Z}$. Observe that for $D \equiv 1 \pmod{4}$ the same need not hold for $m \mid a + b\sqrt{D}$, $a, b \in \mathbb{Z}$.
- Solve the Diophantine equations $x^2 + 1 = y^5$, $x^2 + 3 = y^3$ and $x^2 + 4 = y^3$.
- Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$, resp. $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ for $D \equiv 2, 3$, resp. $1 \pmod{4}$.
- Let $K = \mathbb{Q}(\sqrt{D})$. If $P < \mathcal{O}_K$ is a nonzero prime ideal and $\alpha \in \mathcal{O}_K$, then $\alpha^{NP} \equiv \alpha \pmod{P}$.
- Let R be a Gaussian domain and T its field of fractions. If $u \in T$ is integral over R , then $u \in R$.
- * A prime $p > 5$ is given together with a natural number k such that $p \mid k^2 + 5$. Prove that there exist natural numbers m, n satisfying $p^2 = m^2 + 5n^2$. Assume that you know that the class group of $\mathbb{Z}[\sqrt{-5}]$ has two elements.

12. ** Try to think through that when $D \equiv 1 \pmod{4}$, then $\mathbb{Z}[\sqrt{D}]$ can never be a Gaussian domain.

Hints

- 8. Look at when the minimal polynomial has integer coefficients.
- 10. The rational root theorem.
- 11. Find a (prime) ideal with norm p . What does the class group then say about its square?
- 12. Problem 10. points out something that $\mathbb{Z}[\sqrt{D}]$ does not have.

6. Solutions to the exercises

In the version from the winter semester 2023/2024 by Matěj Doležálek.

6.1 Exercises 1

ideals, operations on ideals, prime ideals, maximal ideals

1. Prove that the union of a chain of (arbitrarily many) ideals $I_1 \subset I_2 \subset I_3 \subset \dots$ is an ideal.

Solution. Let R be the ring and I the union under consideration. For $a, b \in I$, $r \in R$ we have to prove $a \pm b \in I$, $ra \in I$. By the definition of the union, for some indices we must have $a \in I_k$, $b \in I_\ell$. For $m = \max\{k, \ell\}$ we then already have $a, b \in I_m$, so by the definition of an ideal both $a \pm b$ and ra lie in $I_m \subset I$.

2. For ideals I, J define $I + J := \{a + b \mid a \in I, b \in J\}$. Prove that $I + J$ is the smallest ideal in R which contains I and J .

Solution. $I + J$ is an ideal: the sum of generic elements of $I + J$ is

$$(a_1 + b_1) + (a_2 + b_2) = \underbrace{(a_1 + a_2)}_{\in I} + \underbrace{(b_1 + b_2)}_{\in J}.$$

Similarly $r(a + b) = ra + rb \in I + J$. Further, $I + J$ trivially contains both I and J . Conversely, if some ideal K contains both I and J , then by closedness under addition it must contain all $a + b$, hence contain $I + J$.

3. Let R be a ring and M an ideal in R . Prove:

- a) M is maximal if and only if $R = M + aR$ for all $a \in R \setminus M$.
- b) If M is maximal and $a \in R \setminus M$, then there are $m \in M$ and $r \in R$ such that $1 = m + ar$.

Solution. a) $M + aR$ is an ideal strictly larger than M (it additionally has the element a), so by maximality it must already be all of R . In the opposite direction, if $M \subsetneq I \subset R$, then choosing $a \in I \setminus M$ we get $R = M + aR \subset I$, so $I = R$, which gives the maximality of M .

b) The ideal on the left-hand side of $R = M + aR$ contains the one, so it can also be expressed on the right in the form $m + ar$.

4. Let us have ideals I, J, K of a ring R . Prove that $IJ \subset I \cap J$ and $I(J + K) = IJ + IK$. Find an example where $IJ \neq I \cap J$.

Solution. Ideals are closed under multiplication, so for $a \in I$, $b \in J$ in particular $ab \in I$. The ideal IJ is formed by sums of such products, so $IJ \subset I$. Completely analogously $IJ \subset J$, so $IJ \subset I \cap J$.

For $I(J + K) = IJ + IK$ let us prove both inclusions; we consider $a \in I$, $b \in J$, $c \in K$. On the left there is a sum of products of the form $a(b + c)$, on the right some sum of products ab plus a sum of products ac . We can multiply out the products of the form $a(b + c)$ and interpret them as elements of the ideal on the right – that is the inclusion “ $\subset$ ”. For the opposite inclusion we can rewrite each

ab as $a(b + 0)$ and each ac as $a(0 + c)$, producing the forms from the left-hand side – that is the inclusion “ $\supset$ ”.

An example with $IJ \neq I \cap J$: $I = J = (2)$ in $\mathbb{Z}$, where $IJ = (4) \neq (2) = I \cap J$.

5. Determine: $\mathbb{Q}[x]/(x + 2)$, $\mathbb{Q}[x]/(x^2 - 2)$, $\mathbb{Q}[x]/(x^2 - 1)$, $\mathbb{R}[x]/(x^2 - 2)$, $\mathbb{Z}[x]/(x^2 - 2)$.

Solution. We get, in order, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q} \times \mathbb{Q}$, $\mathbb{R} \times \mathbb{R}$ and $\mathbb{Z}[\sqrt{2}]$. Strategy: taking the quotient by an irreducible polynomial = adjoining a root; a product of distinct irreducible polynomials is broken up by the Chinese remainder theorem. E.g. for $\mathbb{Q}[x]/(x^2 - 2)$ we use the homomorphism

$$\begin{aligned}\mathbb{Q}[x] &\rightarrow \mathbb{Q}[\sqrt{2}], \\ f &\mapsto f(\sqrt{2}).\end{aligned}$$

The image is all of $\mathbb{Q}[\sqrt{2}]$ (a preimage of any $a + b\sqrt{2}$ is e.g. $bx + a$), the kernel is $(x^2 - 2)$ (the minimal polynomial of $\sqrt{2}$). The 1st isomorphism theorem gives the result. For $\mathbb{Q}[x]/(x^2 - 1)$ we first have to decompose it into $\mathbb{Q}[x]/(x - 1) \times \mathbb{Q}[x]/(x + 1)$ (Chinese remainder theorem); both factors are then isomorphic to $\mathbb{Q}$. (Alternatively we directly use the homomorphism $\mathbb{Q}[x] \rightarrow \mathbb{Q} \times \mathbb{Q}$, $f \mapsto (f(1), f(-1))$, check that it is onto, and observe that the kernel will be $(x^2 - 1)$.)

In particular, for $\mathbb{Z}[x]/(x^2 - 2)$ it may be technically trickier to formulate correctly that the kernel is exactly $(x^2 - 2)$, where, in contrast to the example over $\mathbb{Q}$, we generate the ideal in the sense of the ring $\mathbb{Z}[x]$. Indeed, if we have the properties of minimal polynomials formulated and proved only over fields (as e.g. in the second-year Algebra course), it need not be immediately clear whether a polynomial $f \in \mathbb{Z}[x]$ vanishing at $\sqrt{2}$, which consequently must be a multiple of $x^2 - 2$ in the sense of the ring $\mathbb{Q}[x]$, is also a multiple of $x^2 - 2$ in the sense of the ring $\mathbb{Z}[x]$. This difficulty can be removed in several ways: e.g. one can refer to Gauss’s lemma – if a *primitive* integer polynomial divides another integer polynomial in the sense of $\mathbb{Q}[x]$, then the quotient necessarily lies in $\mathbb{Z}[x]$. The second possibility is to think it through by hand that if we take the minimal polynomial monic and at the same time integral, everything works as it should: we look at $f \in \mathbb{Z}[x]$ satisfying $f(\sqrt{2}) = 0$ modulo $x^2 - 2$, successively replacing x^k by $2x^{k-2}$, until a linear integer polynomial vanishing at $\sqrt{2}$ remains, and the only such one is 0.

6. Prove that the operations on a factor ring are well defined and that it is a ring (and prove the other things from the lecture that we left as exercises).

Solution. R a ring, I an ideal, $a, b \in R$. We want to check that for $x \in a + I$, $y \in b + I$ we will have $x + y \in (a + b) + I$ and similarly $xy \in ab + I$. To this end we write $x = a + i_1$, $y = b + i_2$ and using the closedness of the ideal under addition and under multiplication by an element of the ring we have

$$\begin{aligned}x + y &= a + i_1 + b + i_2 = (a + b) + \underbrace{(i_1 + i_2)}_{\in I}, \\ xy &= (a + i_1)(b + i_2) = ab + \underbrace{(ai_2 + bi_1 + i_1i_2)}_{\in I}.\end{aligned}$$

7. Prove the 3rd isomorphism theorem: If R is a ring, $I < R$ an ideal and $S \subset R$ a subring, then $S + I$ is a subring in R and $(S + I)/I \simeq S/(S \cap I)$.

Solution. That $S + I$ is a subring is checked routinely (it has a one, it is closed under addition and multiplication). Further, let us aim at using the 1st isomorphism theorem. The projection $\pi: R \rightarrow R/I$, $r \mapsto r + I$ is a surjective homomorphism. Let us restrict it to the subring S and call it φ . For $\varphi(s) = s + I$ to be 0, we must have $s \in I$, so $\text{Ker } \varphi = S \cap I$. In the image there appear exactly the residue classes of the form $s + I$, so $\text{Im } \varphi = (S + I)/I$ (one inclusion is obvious; for the other, realize that anything of the form $s + i + I$ is simply the same as $s + I$). The 1st isomorphism theorem then gives the result.

8. Consider the ring $\mathbb{Z}$ and the ideals $I = (168)$ and $J = (288)$ in it.

- a) What do all maximal ideals and prime ideals in $\mathbb{Z}$ look like?
- b) Determine $I + J$, IJ , $I \cap J$, $I^2 + J$.
- c) Find all prime ideals which contain the ideal I , J , IJ , $I \cap J$, resp. J^2 .

Solution. a) The principal ideals generated by primes (and, among the prime ideals, also (0)).

b) See part a) of the following problem; we get $I + J = (24)$, $IJ = (48384)$, $I \cap J = (2016)$, $I^2 + J = (288)$.

c) The prime ideals containing (x) , $x \neq 0$, correspond to the primes dividing x . So it suffices to use $168 = 2^3 \cdot 3 \cdot 7$, $288 = 2^5 \cdot 3^2$ and always to take the primes from the factorization.

9. Let R be a principal ideal domain and $a, b \in R$.

- a) Determine $(a)(b)$, $(a) + (b)$, $(a) \cap (b)$.
- b) What do all maximal ideals and prime ideals in R look like?
- c) Prove that the factor of R by a nonzero prime ideal is a field.

Solution. a) $(a)(b) = (ab)$, $(a) + (b) = (\gcd(a, b))$, $(a) \cap (b) = (\text{lcm}(a, b))$.

b) The nonzero ones are exactly the principal ideals generated by irreducible elements/prime factors (in a PID irreducible = prime factor); moreover (0) is a prime ideal, since R is a domain. As a consequence of c), the nonzero prime ideals are automatically maximal.

c) Let (p) be a nonzero prime ideal; then p is irreducible. We want every nonzero element of $R/(p)$ to have an inverse. But for $a \notin (p)$ we have $(a) + (p) = (\gcd(a, p)) = (1)$, so $xa + yp = 1$ for some x, y . But then $xa \equiv 1 \pmod{p}$.

10. For subsets A, B of a ring R define $A \odot B := \{ab \mid a \in A, b \in B\}$ (beware, this does not correspond to the multiplication of ideals). Let I be an ideal in R . Prove that $(a+I) \odot (b+I) \subset ab+I$. Does the opposite inclusion hold?

Solution. The inclusion to be proved is simply the fact that multiplication of elements in the factor ring modulo I works. The opposite inclusion does not hold: e.g. $2 \cdot 2 + 5\mathbb{Z}$ contains the prime 19, but $(2 + 5\mathbb{Z}) \odot (2 + 5\mathbb{Z})$ does not (the only factorizations $19 = (\pm 1)(\pm 19)$ use factors congruent to $\pm 1 \pmod{5}$).

11. Consider the principal ideal domain $\mathbb{Q}[x]$ and the ideals $I = (x^3 + x^2 + 2x + 2)$ and $J = (x^3 - 2x^2 + 2x - 4)$.

- a) Determine $I + J$, IJ , $I \cap J$, $I^2 + J^3$.
- b) Which factors modulo the principal ideals from part a) are domains?
- c) Find all prime ideals which contain the ideal I , J , IJ , $I \cap J$, resp. J^2 .

Solution. Let us factor the polynomials:

$$x^3 + x^2 + 2x + 2 = (x + 1)(x^2 + 2), \quad x^3 - 2x^2 + 2x - 4 = (x - 2)(x^2 + 2).$$

In a) we thus easily determine the required gcds and lcms:

$$\begin{aligned} I + J &= (x^2 + 2), & IJ &= \left((x^3 + x^2 + 2x + 2) \cdot (x^3 - 2x^2 + 2x - 4) \right), \\ I \cap J &= \left((x + 1)(x - 2)(x^2 + 2) \right), & I^2 + J^3 &= \left((x^2 + 2)^2 \right). \end{aligned}$$

b) A factor is a domain if we take the quotient by a prime ideal, which here corresponds to an irreducible polynomial. Hence only $I + J$; the others are written as products of several polynomials.

c) Again we take all principal ideals generated by the irreducible polynomials from the factorization.

12. Let R be a Noetherian ring and $I < R$ an ideal. Prove that R/I is Noetherian as well.

Solution. For a contradiction, let R/I not be Noetherian. The ideals in R/I are exactly of the form J/I for $J < R$, $J \supset I$, so for R/I to be non-Noetherian we must have an infinite increasing chain

$$J_1/I \subsetneq J_2/I \subsetneq J_3/I \subsetneq \cdots$$

But then $J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$ is an infinite increasing chain of ideals in R as well – a contradiction.

13. We are given a ring R in which for every $x \in R$ there is an integer $n \geq 2$ such that $x^n = x$. Prove that every prime ideal in R is maximal.

Solution. Let $P \leq R$ be a prime ideal and let us look at R/P . We want to show that it is a field, so let $x + P \in R/P$ be an arbitrary nonzero element and let us find its inverse. By assumption, the original representative $x \in R$ satisfied $x^n = x$ for a certain $n \geq 2$. This remains valid in R/P as well, and since P is a prime ideal, we can cancel the element $x + P \neq 0 + P$, so

$$\begin{aligned}(x + P)^n &= x^n + P = x + P, \\ (x + P) \cdot (x + P)^{n-2} &= 1 + P.\end{aligned}$$

So every nonzero element of R/P has an inverse, so R/P is a field, so P is a maximal ideal.

6.2 Exercises 2

Gauss's lemma, the Chinese remainder theorem, applications of Zorn's lemma

1. Let R be a Gaussian domain and T its field of fractions. For every irreducible polynomial $f \in T[x]$ there is $u \in T \setminus \{0\}$ such that uf is an irreducible element of $R[x]$.

Solution. We take $u := \prod_p p^{-c_p(f)}$. This product makes sense, because only finitely many prime factors p can give a nonzero content of the polynomial, since in each denominator of each coefficient only finitely many prime factors take part. Then we get $c_p(uf) = v_p(u) + c_p(f) = 0$ for every p , so $uf \in R[x]$ is primitive. Since it is at the same time irreducible in $T[x]$, it is irreducible in $R[x]$ by Gauss's lemma (in the form of Proposition 1.16b)).

2. Let K be a field. Then $K[x, y]$ and $K[x_1, x_2, \dots]$ (infinitely many variables) are Gaussian, but $K[x, y]$ is not a principal ideal domain (though it is Noetherian) and $K[x_1, x_2, \dots]$ is neither Noetherian nor a principal ideal domain.

Solution. From Gauss's lemma we have " R Gaussian $\implies R[x]$ Gaussian". We know that $K[x]$ is a PID, hence Gaussian, so $K[x, y] \simeq K[x][y]$ is Gaussian as well.

Similarly every $K[x_1, \dots, x_n]$ is Gaussian. We use this for $K[x_1, \dots]$: each of its elements f uses only finitely many variables, so it itself lies in some $K[x_1, \dots, x_n]$. That is Gaussian, so there we have a unique factorization. Moreover, we know that no factorization using some further variable can work – we would necessarily have a positive degree with respect to it, whereas f has degree zero with respect to x_i , $i > n$. The unique factorization of f in $K[x_1, \dots, x_n]$ thus remains unique in $K[x_1, \dots]$.

$K[x, y]$ is not a PID, because (x, y) , i.e. the ideal generated by the elements x and y , cannot be principal. Indeed, if $(x, y) = (f)$ for some $f \in K[x, y]$, we would have $f \mid x$, so $\deg_y(f) \leq \deg_y(x) = 0$, i.e. f is constant with respect to y . Completely analogously, f is constant with respect to x . So it is a constant $f \in K$, which is a contradiction, because no constants lie in (x, y) (each term contains x or y in a positive power). All the more, $K[x_1, x_2, \dots]$ cannot be a PID either.

Noetherianity: Hilbert's basis theorem says " R Noetherian $\implies R[x]$ Noetherian". A field K is trivially Noetherian (it has only two ideals), so $K[x]$ is Noetherian, so $K[x, y] \simeq K[x][y]$ is Noetherian. On the other hand, $K[x_1, x_2, \dots]$ is not Noetherian, because we have the chain of ideals

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots \subsetneq (x_1, \dots, x_n) \subsetneq \cdots$$

3. Describe all ideals in the ring $\mathbb{Z}/(150)$ and characterize which pairs of them are comaximal.

Solution. The ideals in $\mathbb{Z}/(150)$ are of the form $I/(150)$, where I are the ideals $(150) \subset I < \mathbb{Z}$. Since $\mathbb{Z}$ is a PID, these I are exactly of the form (d) for $d \mid 150 = 2 \cdot 3 \cdot 5^2$. Two such $I_1/(150)$, $I_2/(150)$ are comaximal if and only if I_1, I_2 are comaximal in $\mathbb{Z}$, which happens when their generators $(I_1 = (d_1), I_2 = (d_2))$ are coprime – so e.g. $(2)/(150)$ and $(3)/(150)$ or $(6)/(150)$ and $(25)/(150)$.

4. Let R be a ring. Using Zorn's lemma, prove that every proper ideal is contained in some maximal ideal.

Solution. Let an ideal $I \subsetneq R$ be given. Consider

$$\mathcal{A} := \{\text{ideal } J \mid I \subset J \subsetneq R\}$$

ordered by inclusion. Obviously $I \in \mathcal{A}$, so this partially ordered set is non-empty. Whenever $\mathcal{B} \subset \mathcal{A}$ is a non-empty chain, put $\tilde{J} := \bigcup \mathcal{B}$. That is an ideal (see the first exercise sheet) and it obviously contains I . If it were not proper, then it would contain 1, so 1 would have to lie already in some $J \in \mathcal{B}$, which is impossible. Hence $\tilde{J} \in \mathcal{A}$ (and the empty chain has the upper bound I). This verifies the conditions of Zorn's lemma, so we have some maximal M in $\mathcal{A}$.

We claim that it is a maximal ideal. If it were not, then there is some ideal I' with $M \subsetneq I' \subsetneq R$. But then I' would be proper and would contain I , so $I' \in \mathcal{A}$, which contradicts the maximality of M . So M is indeed a maximal ideal containing I .

5. Use the proof of the Chinese remainder theorem (in particular the step where $1 = a_1 + a_2$) to construct an explicit isomorphism $\mathbb{Z}/(n) \times \mathbb{Z}/(m) \simeq \mathbb{Z}/(mn)$ for $n = 16, m = 35$. Which well-known theorem does the step in parentheses correspond to?

Solution. One direction of the isomorphism $\mathbb{Z}/(mn) \rightarrow \mathbb{Z}/(n) \times \mathbb{Z}/(m)$ is trivial:

$$z + (mn) \mapsto (z + (n), z + (m)).$$

To find the opposite isomorphism $(a + (n), b + (m)) \mapsto ??? + (mn)$, we need $z_1 + (mn) \in \mathbb{Z}/(mn)$ such that $z_1 \mapsto (1, 0)$, and similarly some $z_2 \mapsto (0, 1)$. For this Bézout's theorem is useful, because if $xn + ym = 1$, then it suffices to take $z_1 = ym$ and $z_2 = xn$.

So we run the extended Euclidean algorithm on $n = 16$ and $m = 35$:

$$\begin{array}{r|rr} 35 & 1 & 0 \\ 16 & 0 & 1 \\ \hline 2 & 3 & 1 \quad -2 \\ 5 & 1 & -5 \quad 11 \end{array}$$

Hence $11 \cdot 16 + (-5) \cdot 35 = 1$. So we take $z_1 = (-5) \cdot 35 = -175$, $z_2 = 11 \cdot 16 = 176$, which gives the explicit isomorphism

$$\begin{aligned} \mathbb{Z}/(n) \times \mathbb{Z}/(m) &\rightarrow \mathbb{Z}/(mn), \\ (a + (n), b + (m)) &\mapsto -175a + 176b + (mn). \end{aligned}$$

(Bézout's coefficients are not unique at all, so as integers we could choose other numbers here as well; nevertheless their residue classes mod (mn) should still be the same.)

6. Realize that in an ordered set $\mathcal{A}$ there can also exist an uncountable chain $\mathcal{B}$ for whose indexing the natural numbers are not enough. Find a couple of examples of such a situation. (There is no catch in it; it is just so that one does not get the impression that in Zorn's lemma it suffices to deal with chains indexed by natural numbers.)

Solution. For example the real numbers with any ordering, or the power set of $\mathbb{R}$ ordered by inclusion, or anything else. Gourmets can also imagine their favourite monstrously large cardinal or ordinal.

7. Show that if $\varphi : R \rightarrow S$ is a ring homomorphism, then the relations $\psi(r) := \varphi(r)$ for $r \in R$ and $\psi(x) := x$ are satisfied by exactly one homomorphism $\psi : R[x] \rightarrow S[x]$. Moreover, ψ is injective/surjective if and only if φ is injective/surjective.

Solution. For a general $f = \sum_{i=0}^d r_i x^i \in R[x]$ we simply put

$$\psi(f) = \sum_{i=0}^d \varphi(r_i) x^i.$$

That ψ respects addition is straightforward; multiplication is somewhat less straightforward, but still easy (the coefficients of products of polynomials are some expressions involving multiplication and addition, which the homomorphism φ both preserves). Since we just apply φ “coefficientwise”, the preservation of injectivity/surjectivity is also clear.

8. Let R be a ring and $I_1, \dots, I_n$ pairwise comaximal ideals in R . Realize that from the CRT we have in particular an isomorphism of multiplicative groups $(R/(I_1 \cdots I_n))^\times \simeq (R/I_1)^\times \times \cdots \times (R/I_n)^\times$. As an application of this fact, think about why for odd primes $p \neq q$ the group $(\mathbb{Z}/(pq))^\times$ cannot be cyclic.

Solution. The ring structure already contains the structure of the multiplicative group, so their isomorphism is just a weakening of the full CRT. Next, the order of $(a, b) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$ is the least common multiple of the orders of a and b . Because of $\gcd(p-1, q-1) \geq 2$ the order then cannot reach $(p-1)(q-1)$.

9. Prove using Zorn’s lemma: in a vector space, any linearly independent set can be extended to a basis.

Solution. Consider the linearly independent supersets of the given set ordered by inclusion and use Zorn’s lemma. A maximal one among them must also be generating, otherwise it would not be maximal.

10. Let $(M, \leq)$ be a partially ordered set. Prove using Zorn’s lemma that the ordering $\leq$ can be extended to a linear ordering, i.e. that there is an ordering $\preceq$ on M which is linear and satisfies: $x \leq y \Rightarrow x \preceq y$ for all $x, y \in M$.

Solution. A partial ordering is a relation, i.e. some subset of $M \times M$, so the orderings themselves can be ordered by inclusion. So let us have

$$\mathcal{A} := \{\preceq \supset \leq \mid \preceq \text{ is a partial ordering of the set } M\}.$$

Similarly as in the previous examples we verify the conditions of Zorn’s lemma; the upper bound of a chain is always its union. Then we have some maximal $\preceq$ in $\mathcal{A}$. For a contradiction, let it not be linear, i.e. let there be some incomparable pair x, y in it, so that neither (x, y) nor (y, x) is an element of $\preceq$. Then we can choose to make y larger than x and add this relation together with all its immediate consequences of transitivity. Formally speaking, we take

$$\widetilde{\preceq} := \preceq \cup \{(a, b) \mid a, b \in M, a \leq x, y \leq b\}$$

and we claim that this is again a partial ordering, which will contradict the maximality of $\preceq$.

- Reflexivity: clear, all pairs (m, m) were already in $\preceq$.
- Antisymmetry: for it to fail, some (b, a) would have to lie already in $\preceq$. But then, thanks to $y \preceq b \preceq a \preceq x$, y and x would have to be comparable, which is a contradiction.
- Transitivity: for it to fail, we must have some $k, \ell, m \in M$ such that $k \preceq \ell$, $\ell \preceq m$, but not $k \preceq m$. If we use only comparisons that were already in $\preceq$, nothing has changed, so WLOG let us assume that $(k, \ell) \in \widetilde{\preceq}$ is one of the pairs of the form (a, b) that we added, i.e. $k \leq x$

and $y \trianglelefteq \ell$. Where does the pair $(\ell, m) \in \widetilde{\trianglelefteq}$ come from? If already $\ell \trianglelefteq m$, then we simply have $y \trianglelefteq \ell \trianglelefteq m$, so $y \trianglelefteq m$, so (k, m) will also be one of the pairs that we added to $\widetilde{\trianglelefteq}$. On the other hand, if (ℓ, m) were to be one of the pairs that we added, this means $\ell \trianglelefteq x$ and $y \trianglelefteq m$. But we already had $y \trianglelefteq \ell$ as well, so altogether $y \trianglelefteq \ell \trianglelefteq x$, which means that x, y were comparable.

11. Let R be a Gaussian domain and T its field of fractions. Let us have a non-constant primitive polynomial $f \in R[x]$. Then f is irreducible in $T[x]$ if and only if it is irreducible in $R[x]$.

Solution. See Proposition 1.16b) in the notes.

12. * Let F be a finite field. Show that any map $g : F \rightarrow F$ can be written as a polynomial.

Solution. The polynomials $x - a$ for $a \in F$ are pairwise coprime. So we can use the Chinese remainder theorem: if we impose the congruences $f \equiv g(a) \pmod{x - a}$, there will be a polynomial satisfying all of them. But $f \equiv f(a) \pmod{x - a}$, so such a polynomial will agree with g at all points.

13. * (Eisenstein's criterion) Let us have a primitive polynomial $f = a_n x^n + \cdots + a_1 x + a_0$ with integer coefficients and a prime p . Prove that if $p \nmid a_n$, $p \mid a_i$ for $i = 0, 1, \dots, n - 1$ and $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Z}$. Try to think about a generalization for a general integral domain R instead of $\mathbb{Z}$.

Solution. For a contradiction f is reducible, i.e. $f = gh$. Then g and h must be primitive, so for reducibility they must be non-constant. We reduce everything modulo p ; the images of our polynomials (in $\mathbb{Z}_p[x]$) will be denoted by a tilde. Then $\tilde{f} = \tilde{g}\tilde{h}$. But by the assumptions $\tilde{f} = a_n x^n$. We know that $\mathbb{Z}_p[x]$ is Euclidean, hence a PID, hence Gaussian, so from unique factorizations we must have $\tilde{g} = b_k x^k$, $\tilde{h} = c_\ell x^\ell$, where $k + \ell = n$. From non-constancy further $k, \ell \geq 1$. But then p divided both constant terms in g and h , so a_0 must be a multiple of p^2 – that is a contradiction.

14. * Using Zorn's lemma, prove that if a ring R has a proper ideal which is not finitely generated, then it also has a prime ideal which is not finitely generated.

Solution. In the standard way, using Zorn's lemma we construct an ideal which is maximal *among those ideals that are not finitely generated*; let us call it P . Then it remains to prove that this ideal is a prime ideal. To this end we need to proceed by contradiction and use the fact that every larger ideal must already be finitely generated. Here is an outline of the proof following this (<https://math.stackexchange.com/a/146899>) answer on stackexchange – thinking through the individual steps is left to the reader:

- 1) If, for a contradiction, P is not a prime ideal, take $x, y \in R$ such that $xy \in P$, but $x, y \notin P$.
- 2) $P + (y)$ is above P , so it is already finitely generated: $P + (y) = (p_1 + r_1 y, \dots, p_n + r_n y)$ with $p_i \in P$.
- 3) $P_y := \{s \in R \mid sy \in P\}$ is an ideal and it lies above P , so again $P_y = (s_1, \dots, s_m)$.
- 4) Take an arbitrary $p \in P$ and express it as an element of $P + (y)$ by means of the generators.
- 5) Express the corresponding linear combination of $r_1, \dots, r_n$ as an element of P_y by means of the generators.
- 6) $P = (p_1, \dots, p_n, s_1 y, \dots, s_m y)$, a contradiction.

6.3 Exercises 3

root fields and splitting fields, algebraic closure, the Galois group, separability

1. Let α be an algebraic element over a field T . Then $[T(\alpha) : T] = \deg m_{\alpha, T}$.

Solution. Let $n := \deg m_{\alpha, T}$. I claim that $1, \alpha, \dots, \alpha^{n-1}$ is a basis of $T(\alpha)$ as a vector space over T . That it is a generating set: it suffices to generate any power α^k . For $k \leq n-1$ we can do that trivially. The minimal polynomial says that

$$\alpha^n + (\text{some linear combination of } 1, \dots, \alpha^{n-1}) = 0,$$

so $\alpha^n =$ some linear combination of $1, \dots, \alpha^{n-1}$, so we can rewrite every higher power of α as a linear combination of lower ones – by sufficiently many repetitions we obtain a linear combination of $1, \dots, \alpha^{n-1}$. That it is a linearly independent set: a T -linear combination of $1, \dots, \alpha^{n-1}$ is just the value of some polynomial of degree $\leq n-1$ at α . If it is a nontrivial combination (not all zeros), then it is a nonzero polynomial, so by the minimality of $m_{\alpha, T}$ it cannot have α as a root.

2. For a field T and a polynomial $f(x)$ determine all possible root fields for f over T , the splitting field for f over T , the degrees of all these field extensions and also their Galois groups over T :

$$\text{a) } f(x) = x^2 + 3, T = \mathbb{R}, \quad \text{b) } f(x) = x^2 - 1, T = \mathbb{Q}, \quad \text{*c) } f(x) = x^3 - 2, T = \mathbb{Q}.$$

Solution.

a) The roots of $x^2 + 3$ are $\pm\sqrt{-3}$. We have $\mathbb{R}(\sqrt{-3}) = \mathbb{R}(-\sqrt{-3}) = \mathbb{C}$, so $\mathbb{C}$ is the root field and at the same time the splitting field. $x^2 + 3$ is quadratic and has no root in $\mathbb{R}$, so it is irreducible. $\mathbb{C} \supset \mathbb{R}$ then, as a root field of a quadratic irreducible polynomial, has degree 2.

$\text{Gal}(\mathbb{C}/\mathbb{R})$ has two elements: one automorphism is the identity, the other the complex conjugation $z \mapsto \bar{z}$. That these are automorphisms: for id it is trivial; for complex conjugation we know e.g. from algebra that it respects addition and multiplication, fixes the real numbers and moreover is a bijection, so it is indeed an $\mathbb{R}$ -automorphism of the field $\mathbb{C}$. That no further automorphisms exist: we know that in an extension of degree 2 the Galois group must embed injectively into S_2 . But that is a two-element group, so we cannot have more than two elements in $\text{Gal}(\mathbb{C}/\mathbb{R})$.

b) f has the roots ± 1 , which are both elements of $\mathbb{Q}$. The root field and the splitting field is thus only $\mathbb{Q}$ itself, the degree of the extension is 1 and the Galois group is trivial.

c) This part is already harder and will be solved more easily with more advanced tools from the lecture. So, without proof: there are three root fields – $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2})$, $\mathbb{Q}(e^{\frac{-2\pi i}{3}}\sqrt[3]{2})$. Each is of degree 3 (root extensions of an irreducible polynomial of degree 3), but their Galois groups are trivial. The splitting field is $\mathbb{Q}(e^{\frac{2\pi i}{3}}, \sqrt[3]{2})$ and it has degree six. Its Galois group has six elements and is isomorphic to S_3 . It can be generated by two elements, one of which fixes $\sqrt[3]{2}$ and complex-conjugates $e^{\frac{2\pi i}{3}}$ to $e^{\frac{-2\pi i}{3}}$, while the other fixes $e^{\frac{2\pi i}{3}}$ and rotates $\sqrt[3]{2}$ to $e^{\frac{2\pi i}{3}}\sqrt[3]{2}$.

3. Let us have fields $T \subset U \subset V$. If V is algebraic over U and U is algebraic over T , then V is also algebraic over T .

Solution. First the baby version, when the extensions are moreover finite (a finite extension is necessarily algebraic – see 5.). Then we can simply say that

$$[V : T] = [V : U] \cdot [U : T]$$

is finite, so $V \supset T$ is algebraic.

Now the grown-up version with potentially infinite extensions. We take $\alpha \in V$ and show that it is algebraic over T . We know that it is algebraic over U , so it is a root of some

$$f = u_n x^n + \dots + u_1 x + u_0 \in U[x].$$

Obviously α is then also algebraic over $T(u_n, \dots, u_1, u_0)$. Then $T(\alpha, u_n, \dots, u_0)$ is algebraic over $T(u_n, \dots, u_0)$, which is algebraic over T (since it is a subfield of U). But these are certainly finite extensions, so by the baby version $T(\alpha, u_n, \dots, u_0)$ is an algebraic extension of T , so α is algebraic over T .

4. Let $U \supset T$ be a field extension and $\alpha \in U$ a root of *some* separable $f \in T[x]$. Then α is separable over T .

Solution. $m_{\alpha,T} \mid f$. Now if $m_{\alpha,T}$ had a multiple root in $\overline{T}$, then by divisibility f would have it as well, a contradiction.

5. A field extension of finite degree is necessarily algebraic.

Solution. Let $[U : T] < \infty$. But then for every $a \in U$ we have $T(a) \subset U$, so

$$[T(a) : T] \leq [U : T] < \infty,$$

which means that a is algebraic over T .

6. Let us have field extensions $V \supset U \supset T$. Then $[V : T] = [V : U] \cdot [U : T]$.

Solution. Let $n := [U : T]$, $m := [V : U]$. Further choose $\{u_i\}_{i=1}^n$ a basis of U as a vector space over T and $\{v_j\}_{j=1}^m$ a basis of V as a vector space over U . I claim that $\{u_i v_j\}_{\substack{i=1,\dots,n \\ j=1,\dots,m}}$ is a basis of V as a vector space over T . That it is generating: any $v \in V$ we first express as

$$v = \sum_{j=1}^m \alpha_j \cdot v_j,$$

where α_j are coefficients belonging to U . Each of them can therefore be expressed as

$$\alpha_j = \sum_{i=1}^n \beta_{i,j} u_i,$$

so that we subsequently have

$$v = \sum_{i=1}^n \sum_{j=1}^m \beta_{i,j} \cdot u_i v_j.$$

That it is independent: let

$$0 = \sum_{i=1}^n \sum_{j=1}^m \beta_{i,j} \cdot u_i v_j$$

and let us show that all $\beta_{i,j}$ must be zero. In the sum we can collect $\alpha_j := \sum_{i=1}^n \beta_{i,j} u_i \in U$; then we have $0 = \sum_{j=1}^m \alpha_j v_j$, which by the linear independence of the basis $\{v_j\}$ means $\alpha_1 = \dots = \alpha_m = 0$. Similarly, for every $j = 1, \dots, m$, $0 = \sum_{i=1}^n \beta_{i,j} u_i$ means, thanks to the linear independence of $\{u_i\}$, that all $\beta_{i,j}$ are zero.

7. Let $T \subset U$ be an algebraic field extension and $U \subset K$ (not necessarily algebraic). Then K is an algebraic closure of U if and only if K is an algebraic closure of T .

Solution. Being an algebraic closure of a field means being its algebraic extension and at the same time being algebraically closed. Algebraic closedness is just a property of the field K , which does not depend on over which smaller field we look at it. As a consequence of **3.**, further $K \supset T$ is algebraic if and only if $K \supset U$ is algebraic.

8. Let $\varphi : K \rightarrow R$ be a ring homomorphism. Recall that when K is a field, φ must be injective.

Solution. $\text{Ker } \varphi$ is an ideal in K , but fields have only two ideals (the zero ideal and the whole field). Moreover, by the definition of a ring homomorphism, $\varphi(1_K) = 1_R$, so $1 \notin \text{Ker } \varphi$, hence $\text{Ker } \varphi = 0$.

9. For a field T and a polynomial $f(x)$ determine all possible root fields for f over T , the splitting field for f over T , the degrees of all these field extensions and (possibly) also their Galois groups over T :

- a) $f(x) = x^2 + 1$, $T = \mathbb{Q}$,
 b) $f(x) = x^4 - 1$, $T = \mathbb{Q}$,
 *c) $f(x) = x^2 + 1$, $T = \mathbb{Z}_7$,
 **d) $f(x) = x^n - 1$, $T = \mathbb{Q}$, $n \in \mathbb{N}$.

Solution. a) root field = splitting field = $\mathbb{Q}(i)$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\text{id}, (z \mapsto \bar{z})\} \simeq \mathbb{Z}_2$.

b) The root field can be $\mathbb{Q}(1) = \mathbb{Q}(-1) = \mathbb{Q}$ (degree of the extension 1, trivial Galois group), or $\mathbb{Q}(i) = \mathbb{Q}(-i)$, which we have already seen. The splitting field is $\mathbb{Q}(i)$.

c) The root field and the splitting field is $\mathbb{Z}_7(i)$. What does this mean? Simply, to $\mathbb{Z}_7$, where the polynomial $x^2 + 1$ had no root, we add an element i , to which we assign the property $i^2 = -1$. The result is a field with $7^2 = 49$ elements. The degree of the extension is 2, the Galois group has two elements (the identity and the “complex conjugation” $a + bi \mapsto a - bi$ for $a, b \in \mathbb{Z}_7$).

d) Let $\zeta_n := e^{\frac{2\pi i}{n}}$. Then the root fields are all $\mathbb{Q}(\zeta_n^j)$. All of this is contained in $\mathbb{Q}(\zeta_n)$, which is thus the splitting field. (For j not coprime to n , $\mathbb{Q}(\zeta_n^j)$ may be different from $\mathbb{Q}(\zeta_n)$, so for “highly composite” n we can get many mutually non-isomorphic root extensions.)

Determining the degrees in full generality is hard: there is the (hard) theorem saying that the minimal polynomial of ζ_n (the so-called n -th cyclotomic polynomial) has degree $\varphi(n)$, from which it follows that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Moreover, then $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

10. Let $S \supset T$ be fields, S algebraically closed and $U = \{\alpha \in S \mid \alpha \text{ algebraic over } T\}$. Then U is an algebraic closure of T . (Proposition 2.8 of the notes)

Solution. The proof is in the notes...

11. Let T, U be fields of characteristic 0. Then $\mathbb{Q} \subset T, U$ and every homomorphism $\varphi : T \rightarrow U$ is a $\mathbb{Q}$ -homomorphism. (In characteristic p the field $\mathbb{Z}_p$ has the same property.)

Solution. By the definition of a homomorphism we must have $\varphi(1) = 1$. Then we also easily get $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1+1 = 2$; in this way by induction we get $\varphi(n) = n$ for all natural n . Further we know $0 = \varphi(0) = \varphi(n + (-n)) = \varphi(n) + \varphi(-n) = n + \varphi(-n)$, so necessarily $\varphi(-n) = -n$. Hence we have $\varphi(n) = n$ for every integer n . Then for $\frac{p}{q} \in \mathbb{Q}$ we similarly get

$$p = \varphi(p) = \varphi\left(q \cdot \frac{p}{q}\right) = \varphi(q) \cdot \varphi\left(\frac{p}{q}\right) = q \cdot \varphi\left(\frac{p}{q}\right),$$

so $\varphi\left(\frac{p}{q}\right) = \frac{p}{q}$. Hence φ indeed fixes all rational numbers.

12. An element α is algebraic over a field T if and only if $T(\alpha) = T[\alpha]$.

Solution. Let $\beta \in T[\alpha]$ be nonzero; β is algebraic as well, since $T[\alpha]$ has finite dimension over T . Then its minimal polynomial $m_{\beta,T}$ has a nonzero constant term (otherwise $x \mid m_{\beta,T}$), so

$$m_{\beta,T}(x) = \sum_{i=0}^n b_i x^i,$$

where $b_0 \neq 0$. But then we can rearrange to $\frac{1}{\beta} = -\frac{1}{b_0} \sum_{i=1}^n b_i \beta^{i-1}$. Similarly, conversely, from an expression of the inverse we get back a minimal polynomial.

13. * No finite field is algebraically closed.

Solution. Let us have a finite field F and let $n := |F|$. Its multiplicative group has $n - 1$ elements, so by Lagrange's theorem $a^{n-1} = 1$ for $a \in F \setminus \{0\}$. From this we deduce that $a^n = a$ for every $a \in F$. So the polynomial $x^n - x$ has every element of F as a root, which however means that the polynomial $x^n - x + 1$ has no roots in $F - F$ thus cannot be algebraically closed.

14. * Let p be a prime, $T = \mathbb{Z}_p(y)$ and $U = T(\sqrt[p]{y})$. Determine $[U : T]$, $[U : T]_s$ and $\text{Gal}(U/T)$.

Solution. $\sqrt[p]{y}$ is a root of $x^p - y$, which is irreducible using Eisenstein's criterion over the PID $\mathbb{Z}_p[y]$ (with the help of Gauss's lemma one gets the irreducibility over $\mathbb{Z}_p(y)$ as well), so it is already the minimal polynomial. Hence directly $[U : T] = p$. But $x^p - y = (x - \sqrt[p]{y})^p$ (in characteristic p raising to the p -th power is a homomorphism), so this minimal polynomial has only one unique root. Any T -homomorphism $U \rightarrow \bar{T}$ must thus send $\sqrt[p]{y}$ again to $\sqrt[p]{y}$, which means that the only such T -homomorphism is the identity. Hence $[U : T]_s = 1$. In view of $[U : T]_s \geq \#\text{Gal}(U/T)$, the Galois group must then be trivial.

15. * The algebraic closure of an infinite field T has the same cardinality as T .

6.4 Exercises 4

separable, normal, simple and Galois extensions

1. Let $U \supset T$ be an extension of finite degree. Prove that it is Galois if and only if $[U : T] = \#\text{Gal}(U/T)$.

Solution. Let us write down a series of inequalities:

$$\begin{aligned} [U : T] &\stackrel{(1)}{\geq} [U : T]_s = \#\{T\text{-homomorphisms } U \rightarrow \bar{T}\} \stackrel{(2)}{\geq} \\ &\stackrel{(2)}{\geq} \#\{T\text{-homomorphisms } U \rightarrow U\} \stackrel{2.26}{=} \#\{T\text{-automorphisms } U \rightarrow U\} = \\ &= \#\text{Gal}(U/T). \end{aligned}$$

One of the later equalities is provided by Proposition 2.26 of the notes (we may use it, because finite degree implies algebraicity). In (1) equality occurs if and only if $U \supset T$ is separable, while in (2) equality occurs if and only if $U \supset T$ is normal. Given that we already have an extension of finite degree, Galoisness occurs exactly when the extension is both separable and normal, i.e. exactly when equalities occur in (1) and (2), i.e. exactly when $[U : T] = \#\text{Gal}(U/T)$.

2. (preservation and composition of distinguished properties) Let $V \supset U \supset T$ be field extensions. If you know that the extension $V \supset T$ has property X , decide whether $V \supset U$ or $U \supset T$ must necessarily have property X as well. If you know that both $V \supset U$, $U \supset T$ have property X , decide whether $V \supset T$ must necessarily have it as well.

- $X =$ of finite degree,
- $X =$ algebraic,
- $X =$ separable,
- $X =$ normal,
- $X =$ Galois.

Solution.

- Both partial extensions must be of finite degree; conversely, if both are, then $V \supset T$ is of finite degree as well.
- Likewise both partial extensions are algebraic and their algebraicity already implies the algebraicity of $V \supset T$ (see the previous exercise sheet).
- Both partial extensions must be separable: $\alpha \in V$ is a root of a separable $f \in T[x]$, which is also $\in U[x]$; whereas $\beta \in U$ is separable over T purely because $\beta \in V$. In the opposite direction: for $[V : T] < \infty$ this easily follows using separability degrees. In the general case, if $\gamma \in V$, then it is separable over U , hence a root of a certain $f = a_n x^n + \dots + a_1 x + a_0 \in U[x]$, so separable over $T(a_0, \dots, a_n)$. We know that both $T(a_0, \dots, a_n) \supset T$ and $T(\gamma, a_0, \dots, a_n) \supset T(a_0, \dots, a_n)$ are separable and of finite degrees, so γ is already separable over T .

- d) $V \supset U$ must be normal (a U -homomorphism is in particular a T -homomorphism), $U \supset T$ not necessarily (e.g. $\mathbb{Q}(\omega, \sqrt[3]{2}) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$). Similarly $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ shows that $V \supset T$ need not be normal, even if both $V \supset U$ and $U \supset T$ are.
- e) We just put together the answers for finite degree, separability and normality. $V \supset U$ must be Galois, $U \supset T$ not necessarily; the converse implication does not hold either (the same counterexamples as for normality).

3. Decide for the following extensions which of the distinguished properties from Problem **2.** they have and which they do not:

- a) $\mathbb{C} \supset \mathbb{R}$, b) $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$, *c) $\mathbb{Z}_p(x) \supset \mathbb{Z}_p$, *d) $\overline{\mathbb{Q}} \supset \mathbb{Q}$.

Solution.

- a) $[\mathbb{C} : \mathbb{R}] = 2$, so it is an extension of finite degree, in particular also algebraic. We get separability for free thanks to characteristic 0, and it is normal e.g. thanks to the fact that $\mathbb{C}$ is the splitting field of the polynomial $x^2 + 1$ over $\mathbb{R}$. Consequently it is also a Galois extension.
- b) The degree is $3 < \infty$, so it is certainly an algebraic extension. Separability is free thanks to the characteristic, but the extension is not normal – the polynomial $x^3 - 2$ has one root in the extension, but the other two not. Consequently the extension cannot be Galois either.
- c) As a vector space over $\mathbb{Z}_p$, already $\mathbb{Z}_p[x]$ has infinite dimension, which can only increase by passing to the field of fractions $\mathbb{Z}_p(x)$. So it is not an extension of finite degree. Further, the element $x \in \mathbb{Z}_p(x)$ is not a root of any nonzero polynomial from $\mathbb{Z}_p[y]$, so it is not an algebraic extension. As a consequence, it does not even make sense to talk about separability or normality, so not about Galoisness either.
- d) The algebraic closure contains all algebraic extensions, and we can certainly construct them arbitrarily large, so we must have $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. (One can, however, think about the fact that the dimension of $\overline{\mathbb{Q}}$ as a vector space over $\mathbb{Q}$ is only countable, because $\overline{\mathbb{Q}}$ itself has only countably many elements.) Directly from the definition of the algebraic closure it must be an algebraic extension. Then it is also separable for free, because of characteristic 0. Normality will also hold trivially: when we unfold the definition of normality, in this case it means whether every $\mathbb{Q}$ -homomorphism (T -homomorphism) $\overline{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}$ (here meant as $U \rightarrow \overline{T}$) is in fact $\overline{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}$ (here meant as $U \rightarrow U$), which holds completely tautologically. So the extension is normal, but it will not be Galois, because it does not have finite degree.

4. Let $V \supset T$ be a Galois extension and $V \supset U \supset T$. Prove that $[U : T] = \frac{\#\text{Gal}(V/T)}{\#\text{Gal}(V/U)}$.

Solution. By **2.e)**, $V \supset U$ is also a Galois extension, so from **1.** we get

$$\frac{\#\text{Gal}(V/T)}{\#\text{Gal}(V/U)} = \frac{[V : T]}{[V : U]} = [U : T].$$

5. Let $f \in T[x]$ be a polynomial with the factorization into mutually non-associated irreducible polynomials $f = f_1 \cdots f_k$. Consider the Galois group of the splitting field of f over T as a group of permutations of the set of roots of f . Show that each of these permutations must have at least k cycles.

Solution. Since the individual f_i are mutually non-associated, their sets of roots A_i are mutually disjoint (indeed, if $\alpha \in A_i \cap A_j$, this already means $m_{\alpha,T} \mid f_i, f_j$). But we know that every T -automorphism permutes the roots of the same irreducible polynomial from $T[x]$ only among themselves. So every element of Gal will permute each A_i only inside A_i . In each A_i at least one cycle must occur (it is a non-empty set), so altogether there will be $\geq k$ cycles.

6. (review from the lecture) Let U be a field, $G < \text{Aut}(U)$ a subgroup and $T \subset U$ a subfield. Then $\text{Gal}(U/\text{Fix}(U, G)) \supset G$ and $\text{Fix}(U, \text{Gal}(U/T)) \supset T$.

Solution. Obvious after unfolding the definitions: e.g. $\text{Fix}(U, \text{Gal}(U/T))$ is the set of those elements $u \in U$ such that $\varphi(u) = u$ for every $\varphi \in \text{Gal}(U/T)$. But the elements of the Galois group leave the elements of T in place, i.e. $\varphi(t) = t$ for every $t \in T$, which already implies $T \subset \text{Fix}(U, \text{Gal}(U/T))$.

7. Let $U \supset T$ be a separable extension of finite degree. Show that there is a field V such that $U \subset V$, $[V : T] \leq ([U : T])!$ and the extension $V \supset T$ is Galois.

Solution. From the lecture, a separable extension of finite degree is simple, so let $U = T(\alpha)$. This is a root field of the polynomial $m_{\alpha, T}$ over T , so let us also consider its splitting field, which we denote by V . That is certainly an extension field of U and it is normal. Let $n = [U : T] = \deg m_{\alpha, T}$. We know that $m_{\alpha, T}$ is separable, because α is separable over T , so $m_{\alpha, T}$ has n distinct roots $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$. All these elements are separable over T , because they have the same (separable) polynomial. So $V = T(\alpha_1, \dots, \alpha_n)$ arises by adding several separable elements, so it is a separable extension of T . Altogether it is thus also of finite degree (we added finitely many algebraic elements), and hence Galois.

Finally let us estimate $[V : T]$. That is the same as $\# \text{Gal}(V/T)$, but this group embeds into the group of permutations of the set $\{\alpha_1, \dots, \alpha_n\}$, which has order $n!$. We can even say

$$[V : T] \mid ([U : T])!.$$

8. By Proposition 2.26, if $U \supset T$ is an algebraic extension, then every T -homomorphism $\varphi : U \rightarrow U$ must even be a T -automorphism. Think about why algebraicity is necessary – for $T = \mathbb{Z}_p$, $U = T(x)$ (the field of rational functions) find a T -homomorphism $\varphi : U \rightarrow U$ which is not a T -automorphism.

Solution. A generic element of U is of the form $\frac{f}{g}$, $f, g \in T[x]$, $g \neq 0$. Let us introduce the homomorphism

$$\begin{aligned} \varphi : U &\rightarrow U, \\ \frac{f}{g} &\mapsto \frac{f(x^2)}{g(x^2)}, \end{aligned}$$

i.e. “instead of x we write x^2 ”. It is easy to see that this does not depend on the particular way of writing the fraction $\frac{f}{g}$ and that it is a homomorphism (substitution preserves the operations). But it is evidently not surjective: $x \in U$ can never be written as a quotient of two polynomials containing only even powers of x : in the equation $f(x^2) = x \cdot g(x^2)$ the left-hand side has even degree, while the right-hand side has odd degree.

9. Let T be a field with $\text{char } T \neq 2$ and $a, b \in T$ elements with $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin T$. Then $[T(\sqrt{a}, \sqrt{b}) : T] = 4$.

* You can try to prove $\text{Gal}(T(\sqrt{a}, \sqrt{b})/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution. Consider $T \subset T(\sqrt{a}) \subset T(\sqrt{a}, \sqrt{b})$. Each time we extend by the square root of something lying in the previous field, so each of the degrees of the two partial extensions is either 2 or 1. To show that both are 2, it suffices to see that $\sqrt{a} \notin T$ and $\sqrt{b} \notin T(\sqrt{a})$. The first non-membership we have directly from the assumptions; for the second assume, for a contradiction, that $\sqrt{b} = u + v\sqrt{a}$ for some $u, v \in T$. By manipulations we then have

$$\begin{aligned} \sqrt{b} - v\sqrt{a} &= u, \\ b - 2v\sqrt{ab} + v^2a &= u^2, \\ 2v\sqrt{ab} &= b + v^2a - u^2. \end{aligned}$$

Let us distinguish two cases: if $v = 0$, then by the expression $\sqrt{b} = u$ we would in fact have $\sqrt{b} \in T$, which is a contradiction. Otherwise $v \neq 0$ and in view of the given characteristic $\neq 2$ we also have $2 \neq 0$, so we get

$$\sqrt{ab} = \frac{b + v^2a - u^2}{2v} \in T,$$

which is again a contradiction.

Altogether we must have had $\sqrt{b} \notin T(\sqrt{a})$, which already implies $[T(\sqrt{a}, \sqrt{b}) : T(\sqrt{a})] = 2$. Hence $[T(\sqrt{a}, \sqrt{b}) : T] = 2 \cdot 2 = 4$.

10. An extension $U \supset T$ is normal if and only if there exists a set $\mathcal{M} \subset T[x]$ such that U is a splitting field of the set $\mathcal{M}$ over T .

11. * (existence of the separable closure) Let $U \supset T$ be a field extension. All the elements $\alpha \in U$ that are separable over T form a subfield of U .

Solution. Put $V := \{\alpha \in U \mid \alpha \text{ is separable over } T\}$. We only want to show that this set is closed under the field operations. So let us have some $\alpha, \beta \in V$. These are separable elements over T , so from the lecture we know that $T(\alpha, \beta) \supset T$ is a separable extension. But then all the possible operations (sums, products, inverses, ...) we can perform with α, β give results lying in $T(\alpha, \beta)$, so they will also be separable, hence they will again lie in V , which is what we wanted.

12. * Let p be a prime, $U = \mathbb{Z}_p(x, y)$, $T = \mathbb{Z}_p(x^p, y^p)$. Prove that the extension $U \supset T$ is not simple.

Solution. Suppose for contradiction that $U = T(f/g)$, where $f, g \in \mathbb{Z}_p[x, y]$, $g \neq 0$. Let us write

$$f = \sum_{i,j \geq 0} c_{ij} x^i y^j,$$

where the coefficients c_{ij} are from $\mathbb{Z}_p$. In characteristic p raising to the p -th power is a homomorphism, so

$$f^p = \sum_{i,j \geq 0} c_{ij}^p (x^p)^i (y^p)^j \in \mathbb{Z}_p[x^p, y^p].$$

Similarly $g^p \in \mathbb{Z}_p[x^p, y^p]$, so $(f/g)^p \in T$. This means that $[U : T] \leq p$.

We show that the degree of the extension is in fact larger. Indeed, x has the minimal polynomial $z^p - x^p$ over $T[z]$ (notationally this may be slightly confusing, but it is just an application of Eisenstein's criterion and Gauss's lemma, which we have already seen several times – because x^p , although from the notational point of view it looks reducible, is a prime element of $\mathbb{Z}_p[x^p, y^p]$). Similarly y will have the minimal polynomial $z^p - y^p$ over $T(x)$, so we get

$$[U : T] = [T(x, y) : T] = [T(x, y) : T(x)] \cdot [T(x) : T] = p^2,$$

which contradicts $[U : T] \leq p$.

6.5 Exercises 5

computing Galois groups, the Galois correspondence

1. Determine the Galois group of $T \supset \mathbb{Q}$ and all fields U , $T \supset U \supset \mathbb{Q}$, if

a) $T = \mathbb{Q}(i, \sqrt{2})$,

b) T = the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

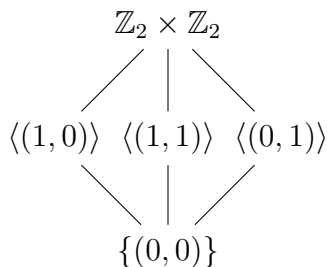
Solution. a) Clearly $[T : \mathbb{Q}] = [T : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$; moreover it is the splitting field of the polynomial $(x^2 - 2)(x^2 + 1)$, so it is normal, separable (characteristic 0) and of finite degree, hence

Galois. So we immediately know that $\#\text{Gal}(T/\mathbb{Q}) = 4$. At the same time every $\mathbb{Q}$ -automorphism $\varphi \in \text{Gal}(T/\mathbb{Q})$ has two possibilities where to send $\sqrt{2}$ and two where to send i . If 4 automorphisms are really to arise, every combination of these two possibilities must give a valid automorphism, so we have four automorphisms of the form

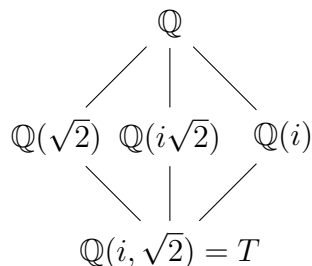
$$\begin{aligned}\sigma_{a,b} : T &\rightarrow T, \\ i &\mapsto (-1)^a i, \\ \sqrt{2} &\mapsto (-1)^b \sqrt{2}\end{aligned}$$

for $a, b \in \mathbb{Z}_2$. It is easy to see that composition will correspond to the addition of the pairs (a, b) in the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, so $\text{Gal}(T/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

To determine the subfields, let us examine the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Clearly, apart from the trivial ones $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\{(0, 0)\}$, we can only have two-element subgroups; but everything except $(0, 0)$ has order 2, so each of the three nonzero elements generates a two-element subgroup. Hence:

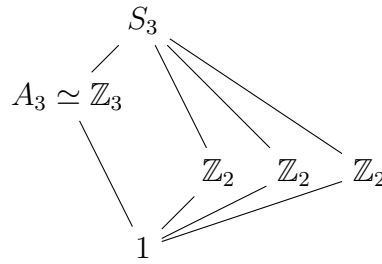


Let us now apply the Galois correspondence; if we keep the orientation of the diagram, then for the resulting fixed fields we shall draw the larger fields lower. For the trivial subgroups we immediately know that the corresponding fixed field must be $\mathbb{Q}$ resp. T , while for the two-element subgroups the fixed field is easy to determine, since being fixed by the identity is trivial, so there always remains just one condition, e.g. $\text{Fix}(T, \langle \sigma_{1,0} \rangle) = \text{Fix}(T, i \mapsto -i) = \mathbb{Q}(\sqrt{2})$, because $\sqrt{2}$ is fixed and it already generates an extension of degree 2, which is what we know should come out. In the same way we obtain the remaining fixed fields:

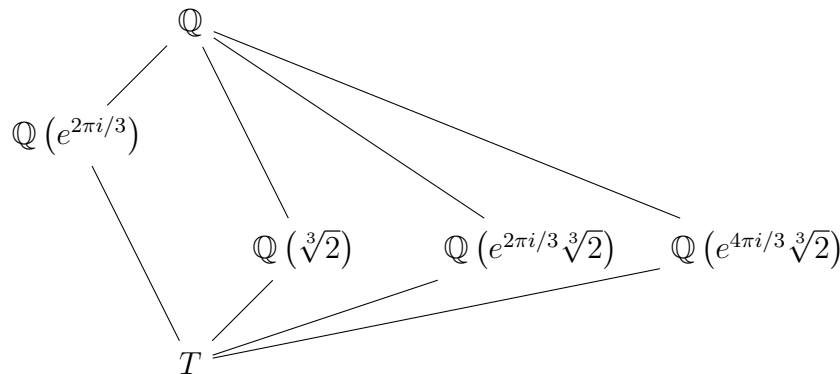


b) In the previous exercise sheets we have already seen that $T = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ and that $[T : \mathbb{Q}] = 6$. It is a Galois extension, and the six-element group $\text{Gal}(T/\mathbb{Q})$ has to embed into S_3 (permutations of the three roots of $x^3 - 2$), so we must already have $\text{Gal}(T/\mathbb{Q}) \simeq S_3$.

S_3 has the following structure of subgroups: the only subgroup of order 3 is the group generated by either of the two 3-cycles, which happens to be the alternating group A_3 as well. Of order 2 there are only the subgroups generated by each of the three transpositions; these are of course isomorphic to $\mathbb{Z}_2$. Schematically we can thus draw:



How do we determine the fixed fields now? The two-element groups are generated by transpositions of two roots and should correspond to a cubic extension – and the field generated by the third root, which the transposition leaves in place, fits exactly. On the other hand, the fixed field of A_3 should be a quadratic extension of $\mathbb{Q}$, and since we know that there should be only one, it suffices to notice the subfield $\mathbb{Q}(e^{2\pi i/3})$. Hence:



2. For the field extension $U \supset T$ determine $[U : T]$ together with a basis of U as a vector space over T , decide whether it is a Galois extension, and if so, determine also all the fields V , $U \supset V \supset T$, if

- | | |
|--|--|
| a) $U = \mathbb{Q}(\sqrt{2}, e^{2\pi i/3}), T = \mathbb{Q},$ | c) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}), T = \mathbb{Q},$ |
| b) $U = \mathbb{Q}(\sqrt[3]{3}), T = \mathbb{Q},$ | d) $U = \mathbb{Q}(\sqrt{1 + \sqrt{2}}), T = \mathbb{Q}.$ |

Solution. I only give the Galois groups and the intermediate fields, provided they are not too complicated.

a) By a trick one can notice that $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$, so $U = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Similarly as in 1.a) we get $\text{Gal}(U/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, and the intermediate fields are $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-6}), \mathbb{Q}(\sqrt{2}, \sqrt{-3})$.

b) It is not Galois, because $x^3 - 3$ has two more complex roots, which will be missing in $U \subset \mathbb{R}$.

c) $\text{Gal}(U/T) \simeq \mathbb{Z}_2^3$. There will be many intermediate fields; if I have not miscounted, seven of degree 2 and seven of degree 4:

$$\begin{aligned} &\mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{5}), \quad \mathbb{Q}(\sqrt{6}), \quad \mathbb{Q}(\sqrt{10}), \quad \mathbb{Q}(\sqrt{15}), \quad \mathbb{Q}(\sqrt{30}), \\ &\mathbb{Q}(\sqrt{3}, \sqrt{5}), \quad \mathbb{Q}(\sqrt{2}, \sqrt{5}), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad \mathbb{Q}(\sqrt{5}, \sqrt{6}), \quad \mathbb{Q}(\sqrt{3}, \sqrt{10}), \quad \mathbb{Q}(\sqrt{2}, \sqrt{15}), \\ &\mathbb{Q}(\sqrt{6}, \sqrt{10}). \end{aligned}$$

d) It is not Galois. Clearly $\sqrt{1 + \sqrt{2}}$ is a root of $(x^2 - 1)^2 - 2$, which under the substitution $x = y + 1$ can be rewritten as $(y^2 + 2y)^2 - 2 = y^4 + 4y^3 + 4y^2 - 2$, and this is irreducible by Eisenstein's criterion with $p = 2$, so $(x^2 - 1)^2 - 2$ must already be the minimal polynomial of $\sqrt{1 + \sqrt{2}}$. But another of its roots is for instance $\sqrt{1 - \sqrt{2}} \notin \mathbb{R}$, whereas $U \subset \mathbb{R}$, which already witnesses that U is not normal.

3. Let U be the splitting field of a polynomial f over a field T . Determine U , $[U : T]$, a basis of U over T and $\text{Gal}(U/T)$ (you may also think about the fields V , $U \supset V \supset T$, but they often look rather ugly), if

- a) $f = x^2 - 5$, $T = \mathbb{Q}$,
 b) $f = x^3 - 2$, $T = \mathbb{Q}(e^{2\pi i/3})$,
 c) $f = (x^2 - 3)(x^2 - 5)$, $T = \mathbb{Q}(\sqrt{2})$,
 *d) $f = (x^2 - 1)^2 - 2$, $T = \mathbb{Q}$.

Solution. a) $U = T(\sqrt{5})$, $[U : T] = 2$, $\text{Gal}(U/T) \simeq \mathbb{Z}_2$, the intermediate fields are only the trivial ones.

b) $U = T(\sqrt[3]{2})$, $[U : T] = 3$, $\text{Gal}(U/T) \simeq \mathbb{Z}_3$, the intermediate fields are only the trivial ones.

c) $[U : T] = 4$, $\text{Gal}(U/T) \simeq \mathbb{Z}_2^2$, the intermediate fields are the trivial ones and $T(\sqrt{3})$, $T(\sqrt{15})$, $T(\sqrt{5})$.

d) $U = T(\sqrt{1 + \sqrt{2}}, i)$, $[U : T] = 8$, $\text{Gal}(U/T) \simeq D_8$, the intermediate fields look complicated, so I take the liberty of omitting them.

4. Let us have fields $V \supset U \supset T$ such that both $V \supset T$ and $U \supset T$ are normal extensions. Then $\text{Gal}(V/U) \triangleleft \text{Gal}(V/T)$ and $\text{Gal}(V/T)/\text{Gal}(V/U) \simeq \text{Gal}(U/T)$.

Solution. Let me additionally assume that $V \supset T$ is a Galois extension (then in particular $U \supset T$ has finite degree). Consider the map defined by restriction

$$\begin{aligned} \text{Gal}(V/T) &\rightarrow \text{Gal}(U/T), \\ \varphi &\mapsto \varphi|_U. \end{aligned}$$

First let me justify that $\varphi|_U$ really is a T -homomorphism $U \rightarrow U$. That it is a T -homomorphism is clear. Then we certainly know at least that it is a T -homomorphism $U \rightarrow \bar{T}$. By the definition of normality it is therefore in fact $U \rightarrow U$. It is a field homomorphism, hence also an injective T -linear map. U has finite dimension over T , so a linear endomorphism is injective if and only if it is surjective, i.e. if and only if it is an automorphism. This proves that $\varphi|_U$ is an automorphism of U .

That the restriction preserves composition of automorphisms is obvious. So we have a group homomorphism. I claim that it is surjective; so let $\varphi \in \text{Gal}(U/T)$ be given and let me find its preimage. Let $V = T(\alpha)$ (a Galois extension, so in particular separable of finite degree). Then V is the splitting field of the polynomial $f := m_{\alpha, T}$ over T . But by Proposition 2.6 of the notes we can extend the T -isomorphism $U =: T_1 \rightarrow T_2 := U$ to some ψ between the splitting fields of the polynomial f resp. $\varphi(f)$. But f has coefficients from T , so $\varphi(f) = f$, and the splitting field of f over U is certainly V (it is already a splitting field over T). So we have extended $\varphi : U \rightarrow U$ to $\psi : V \rightarrow V$, which is what we wanted.

So we have a surjective group homomorphism. What is its kernel? $\varphi|_U = \text{id}_U$ occurs exactly when φ leaves U in place, i.e. $\varphi \in \text{Gal}(V/U)$. The kernel is therefore $\text{Gal}(V/U) \leq \text{Gal}(V/T)$, which immediately makes this subgroup normal, and moreover by the first isomorphism theorem we have

$$\text{Gal}(V/T)/\text{Gal}(V/U) \simeq \text{Gal}(U/T),$$

as we wanted.

5. Let us consider cyclotomic fields.

- a) Recall that $\text{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$. Assume that you already know $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$.
 b) Let U be the splitting field of $x^{20} - 1$ over $\mathbb{Q}(i)$. Determine $\text{Gal}(U/\mathbb{Q}(i))$ and all the intermediate fields V , $U \supset V \supset \mathbb{Q}(i)$.
 c) * Let U be a root field of $x^3 + x^2 - 2x - 1$ over $\mathbb{Q}$. Determine $\text{Gal}(U/\mathbb{Q})$.

Solution. a) Let $\zeta := e^{2\pi i/n}$. We know that this is a root of the n -th cyclotomic polynomial, whose roots are exactly the ζ^k for $k \in \mathbb{Z}_n^*$. From this it follows, on the one hand, that $\mathbb{Q}(\zeta)$ is at the same time a splitting field of the n -th cyclotomic polynomial, so it is a Galois extension of $\mathbb{Q}$. But we also have at most $\varphi(n)$ possible images for ζ , namely the individual ζ^k , $k \in \mathbb{Z}_n^*$, so all these k must give an automorphism. Under composition we see

$$\zeta \mapsto \zeta^{k_1} \mapsto (\zeta^{k_1})^{k_2} = \zeta^{(k_1 k_2)},$$

from which $\text{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$ is immediately visible.

b) We know that $\text{Gal}(U/\mathbb{Q}) \simeq \mathbb{Z}_{20}^*$ and that $\text{Gal}(U/\mathbb{Q}(i))$ is a subgroup of it. So we need the automorphisms given by $\zeta \mapsto \zeta^k$, $k \in \{1, 3, 7, 9, 11, 13, 17, 19\}$, such that $i \mapsto i$. Thanks to $i = \zeta^5$ this means $i^k = i$, i.e. $k \equiv 1 \pmod{4}$, which leaves us with the subgroup $\{1, 9, 13, 17\} \simeq \mathbb{Z}_5^* \simeq \mathbb{Z}_4$ (since $13^2 \equiv 9$, the element 13 must already have order 4). This then has only one nontrivial subgroup $\{1, 9\}$.

I claim that the corresponding fixed field can be described for instance as $\mathbb{Q}(i)(\zeta^4 + \zeta^{-4} - \zeta^8 - \zeta^{-8})$. To see this, notice that $\zeta \mapsto \zeta^9 = -\zeta^{-1}$, so $\zeta^4 \mapsto (-1)^4 \zeta^{-4}$, from which

$$\zeta^4 + \zeta^{-4} - \zeta^8 - \zeta^{-8} \mapsto \zeta^{-4} + \zeta^4 - \zeta^{-8} - \zeta^8$$

is fixed. This expression is in fact equal to $\sqrt{5}$ (one can spot this from what is known about Gauss sums from the second-year Number Theory course¹), so the only nontrivial field lying between U and $\mathbb{Q}(i)$ is $\mathbb{Q}(i, \sqrt{5})$.

c) Denote $\zeta := e^{2\pi i/7}$ and let us look at the problem inside $V := \mathbb{Q}(\zeta)$. I claim that $U = \mathbb{Q}(\zeta + \zeta^{-1})$. That $\zeta + \zeta^{-1}$ is a root of f is verified by substitution, and in the same way one verifies that the other two roots are $\zeta^2 + \zeta^{-2}$ and $\zeta^3 + \zeta^{-3}$. It is also easy to express that these already lie in $\mathbb{Q}(\zeta + \zeta^{-1})$ via

$$\zeta^2 + \zeta^{-2} = (\zeta + \zeta^{-1})^2 - 2, \quad \zeta^3 + \zeta^{-3} = (\zeta + \zeta^{-1})^3 - 3(\zeta + \zeta^{-1}).$$

Then we already see that we have a Galois extension (a splitting field) of degree 3 (it is at the same time a root field, and f is irreducible, e.g. by trying out all the possibilities from the rational root theorem), so we must already have $\text{Gal}(U/\mathbb{Q}) \simeq \mathbb{Z}_3$ (the only three-element group). From this it also follows that U has no nontrivial subfields.

6. Let us have an extension $U \supset \mathbb{Q}$ of finite degree which, however, is not normal. Think about whether we can nevertheless *somehow* use the Galois correspondence to find all the fields V , $U \supset V \supset \mathbb{Q}$. More generally, consider the same for an extension $U \supset T$ which is separable and of finite degree, but is not normal.

Solution. Last time we saw that for a separable extension $U \supset T$ we can find $V \supset U$ such that $V \supset T$ is Galois. Then we can compute $\text{Gal}(V/T)$ and look for subfields of the larger V using the Galois correspondence. Those among them which are even subfields of U will correspond to the overgroups of the subgroup $\text{Gal}(V/U) < \text{Gal}(V/T)$.

7. * Let U be the splitting field of a polynomial f over a field T . Determine U , $[U : T]$, a basis of U over T and $\text{Gal}(U/T)$ and all the fields V , $U \supset V \supset T$, if

- a) $f = x^3 - 5$, $T = \mathbb{Z}_7$,
 b) $f = x^4 - 3$, $T = \mathbb{Z}_5$,
 c) $f = x^{p^k} - x$, $T = \mathbb{Z}_p$.

Solution. a) f has no root in T and it is cubic, so it is already irreducible. Since 1, 2 and 4 are the cube roots of unity in $\mathbb{Z}_7$, if α is a root of f , then so are 2α and 4α , so the root field $\mathbb{Z}_7(\alpha)$ will also be the splitting field U . Hence $[U : T] = 3$, so the Galois group is $\mathbb{Z}_3$ and we have no nontrivial intermediate fields.

b) f has no root in T , and writing out the equations following from a factorisation $x^4 - 3 = (x^2 - ax + b)(x^2 - cx + d)$ shows that no such factorisation exists, so f is irreducible. Now 1, 2, 3, 4 are the fourth roots of unity in $\mathbb{Z}_5$, so for a root α of the polynomial f the multiples of α already represent all the roots, so again the root field $\mathbb{Z}_5(\alpha)$ is at the same time the splitting field. Then we see $[U : T] = 4$. The automorphisms must correspond to $\alpha \mapsto k\alpha$, $k = 1, 2, 3, 4$, which under composition will look like

$$\alpha \mapsto k_1\alpha \mapsto k_1(k_2\alpha) = (k_1k_2)\alpha,$$

¹I would also expect one to see it after staring at a regular pentagon long enough.

from which we see $\text{Gal}(U/T) \simeq \mathbb{Z}_5^* \simeq \mathbb{Z}_4$. The two-element subgroup here is $\{1, 4\}$. The element four corresponds to $\alpha \mapsto 4\alpha = -\alpha$, so α^2 must be fixed by this automorphism. It is a root of the quadratic polynomial $x^2 - 3$, so we indeed obtain a quadratic extension

$$\text{Fix}(U, \{1, 4\}) = \mathbb{Z}_5(\alpha^2).$$

c) In characteristic p the map $a \mapsto a^p$ is a ring homomorphism (it respects both multiplication and addition), so its k -fold composition $a \mapsto a^{p^k}$ will be a homomorphism as well. The set of roots of $f = x^{p^k} - x$ is therefore itself closed under addition, multiplication and multiplicative inverses, so it forms a field. This then has p^k elements, so it is an extension of $\mathbb{Z}_p$ of degree k . The homomorphism $a \mapsto a^p$ is an automorphism, and by composing it we produce k distinct automorphisms (because only the k -fold composition $a \mapsto a^{p^k} = a$ is the identity). This means that the Galois group is cyclic. The subfields are the splitting fields of the polynomials $f_\ell = x^{p^\ell} - x$ for $\ell \mid k$.

8. ** Observe that if $\text{Gal}(T/\mathbb{Q}) \simeq A_4$, then there is no field U , $T \supset U \supset \mathbb{Q}$, with degree $[U : \mathbb{Q}] = 2$. If you feel confident, try to prove that the splitting field of $f = x^4 + 8x + 12$ over $\mathbb{Q}$ is an example of such a T . (I have not managed to prove it so far, but according to a trustworthy source it should be true.)

Solution. By the Galois correspondence the intermediate fields of $T \supset \mathbb{Q}$ correspond to the subgroups of $\text{Gal}(T/\mathbb{Q})$. The degree $[U : \mathbb{Q}] = 2$ would have to correspond to a subgroup of $\text{Gal}(T/\mathbb{Q})$ of index 2, but A_4 has no such subgroup.

A proof that the Galois group A_4 really occurs for the splitting field of $f = x^4 + 8x + 12$ can be found by an eager reader here:

<https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf> (Example 3.3)

6.6 Exercises 6

algebraic sets, Hilbert's Nullstellensatz, radicals

1. Decide which of the following sets are algebraic:

- a) $\{(t, t^2, t^3) \in K^3 \mid t \in K\}$,
- b) $\{(\cos t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$,
- c) $\mathbb{Z}$ as a subset of $\mathbb{R}$,
- d) ${}^*\mathbb{Z}^2$ as a subset of $\mathbb{R}^2$,
- e) ${}^*\{(t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$.

Solution. Everywhere let X denote the given set.

a) I claim $X = V(x^2 - y, x^3 - z)$, which witnesses that X is algebraic. Let us prove the two inclusions. Every point of the form (t, t^2, t^3) will be a zero of both polynomials, because

$$(t)^2 - (t^2) = 0, \quad (t)^3 - (t^3) = 0,$$

so $X \subset V(x^2 - y, x^3 - z)$. For the opposite inclusion, let both polynomials $x^2 - y$, $x^3 - z$ vanish at $(a, b, c) \in K^3$. This means that

$$b = a^2, \quad c = a^3,$$

so if we put $t := a$, then we already have $(a, b, c) = (t, t^2, t^3) \in X$, which proves $X = V(x^2 - y, x^3 - z)$.

b) $X = V(x^2 + y^2 - 1)$, so it is an algebraic set. The inclusion $\subset$ is clear from the Pythagorean identity $(\cos t)^2 + (\sin t)^2 = 1$. For the opposite inclusion, let $(a, b) \in \mathbb{R}^2$ satisfy $a^2 + b^2 - 1 = 0$; then

$$1 = a^2 + b^2 \geq a^2,$$

so $|a| \leq 1$. Hence a lies in the image of the function $\cos : \mathbb{R} \rightarrow [-1, 1]$, so there exists $t \in \mathbb{R}$ such that $a = \cos t$. Then

$$a^2 + (\sin t)^2 = (\cos t)^2 + (\sin t)^2 = 1,$$

so by comparing the equalities $b^2 = (\sin t)^2$. Now if $b = \sin t$, then $(a, b) = (\cos t, \sin t) \in X$; conversely if $b = -\sin t$, then $(a, b) = (\cos(-t), \sin(-t)) \in X$. Altogether this proves $V(x^2 + y^2 - 1) \subset X$ as well.

c) It is not algebraic. Suppose for contradiction that $X = \mathbb{Z} = V(I)$ for some ideal $I \leq \mathbb{R}[x]$. If $I = (0)$, then $V(I) = \mathbb{R} \neq \mathbb{Z}$. So I contains some nonzero polynomial f . The elements of $V(I)$ must then be its roots (not necessarily all the roots, we only have an inclusion), but a nonzero polynomial has only finitely many roots, so $V(I) \subset V(f)$ is finite, which $\mathbb{Z}$ is not, a contradiction.

d) X is not algebraic. If it were, we would have to have $V(I(X)) = X$, so it suffices to show $V(I(X)) \supsetneq X$. Let $f(x, y) \in I(X)$. Consider the polynomial $f(x, 0) \in \mathbb{R}[x]$ arising by substituting zero for y and keeping x as an indeterminate. This polynomial should take the value zero at every integer, so it should have infinitely many roots. But the only polynomial in one variable with infinitely many roots is the zero polynomial, so $f(x, 0) = 0 \in \mathbb{R}[x]$. But this already means that f vanishes on the whole line $\mathbb{R} \times \{0\}$. We did this for an arbitrary $f \in I(X)$, so $\mathbb{R} \times \{0\} \subset V(I(X))$, which already implies $V(I(X)) \supsetneq X$, as we wanted. (By repeated use of the same idea we could even prove $I(X) = (0)$.)

e) X is not algebraic; this can be proved similarly to d). In brief, by considering $f(x, b)$ for constants $b \in [-1, 1]$ we find that anything from $I(X)$ would already vanish on the whole of $\mathbb{R} \times [-1, 1]$, which gives a contradiction with algebraicity. (Similar considerations can be pushed further to show that in fact $I(X) = (0)$.)

2. (a counterexample to Hilbert's theorem without algebraic closedness) Find in $\mathbb{R}[x]$ a maximal ideal which contains no linear polynomial.

Solution. For instance $(x^2 + 1)$ works: the factor ring is $\mathbb{R}[x]/(x^2 + 1) \simeq \mathbb{C}$, which is a field, so it is a maximal ideal. It contains no linear polynomial, however, because a (nonzero) multiple of a quadratic polynomial will have degree ≥ 2 .

3. The *Jacobson radical* of a ring R is defined as $\mathcal{J}(R) := \bigcap_{M < R \text{ maximal}} M$. Observe that $a \in \mathcal{J}(R)$ if and only if $1 - ar$ is a unit for every $r \in R$.

Solution. Firstly, let $a \in \mathcal{J}(R)$ and $r \in R$ be arbitrary, and let us prove that $1 - ar$ is a unit. Suppose for contradiction that $1 - ar$ is not a unit; that means that $(1 - ar)$ is a proper ideal in R . Every proper ideal is contained in some maximal one, so let $(1 - ar) \subseteq M < R$ for M a maximal ideal. But then $1 - ar \in M$ and at the same time $a \in \mathcal{J}(R) \subset M$, hence consequently also $1 = (1 - ar) + r \cdot a \in M$, which is a contradiction. Therefore $1 - ar$ had to be a unit.

Secondly, let $1 - ar$ be a unit for all r , and let us prove that $a \in \mathcal{J}(R) = \bigcap_{M \text{ maximal}} M$. Suppose for contradiction that this is not so, i.e. that there exists a maximal ideal M such that $a \notin M$. That means $a + M \neq 0 + M$ in the factor ring R/M , which by maximality of M is a field. Then there exists $b + M \in R/M$ satisfying $(a + M)(b + M) = 1 + M$, in other words for any representative $b \in R$ we have $1 - ab \in M$. But this already means that with the choice $r := b$ the element $1 - ab$ will not be a unit, because $(1 - ab) \not\subseteq R$.

4. In the domain of the integers $\mathbb{Z}$ determine

- $\sqrt{(0)}, \mathcal{J}(\mathbb{Z})$,
- $\sqrt{(25)}, \sqrt{(125)}, \sqrt{(50)}, \sqrt{(100)}, \sqrt{(\prod_i p_i^{r_i})}$ for pairwise distinct primes p_i .

Further determine

- $\mathcal{J}(\mathbb{Z}/(100))$,
- * when $(\mathbb{Z}/(n))/\mathcal{J}(\mathbb{Z}/(n))$ is a field.

Solution. a) (0) (since $\mathbb{Z}$ is a domain, it certainly has no nilpotent elements other than 0 itself), (0) (a nonzero number cannot be divisible by all primes),

b) $(5), (5), (10), (10), (\prod_i p_i)$. It suffices to prove the last, general form: if $r := \max r_i$, then $(\prod_i p_i)^r \in (\prod_i p_i^{r_i})$, so $(\prod_i p_i) \subset \sqrt{(\prod_i p_i^{r_i})}$; conversely, for $a \in \sqrt{(\prod_i p_i^{r_i})}$, i.e. $a^n \in (\prod_i p_i^{r_i})$, we necessarily must have $p_i \mid a^n$, hence $p_i \mid a$ for all i , so already $a \in (\prod_i p_i)$.

c) $(10)/(100)$, because the only maximal ideals of $\mathbb{Z}/(100)$ are $(2)/(100)$ and $(5)/(100)$.

d) It is precisely for $n = p^k$, p a prime, $k \geq 1$. For it to be a field, $\mathcal{J}(\mathbb{Z}/(n))$ has to be a maximal ideal in $\mathbb{Z}/(n)$, so there must exist exactly one maximal ideal there (because the intersection of two or more maximal ideals can no longer be maximal). The maximal ideals in $\mathbb{Z}/(n)$ correspond to the maximal ideals in $\mathbb{Z}$ containing (n) , i.e. to the primes dividing n , so we need exactly that n be a multiple of only one prime.

5. In the domain $\mathbb{C}[x]$ of polynomials over the complex numbers

- compute $\sqrt{(0)}$, $\mathcal{J}(\mathbb{C}[x])$, $\sqrt{(x-3)^5(x-1)^4(x^3+2)}$, $\sqrt{(x^6-x^4-x^2+1)}$,
- prove that $\sqrt{(p)} = (\frac{p}{\gcd(p,p')})$, where $p \in \mathbb{C}[x]$.

Solution. $\mathbb{C}[x]$ is a principal ideal domain just like $\mathbb{Z}$, so in exactly the same way $\sqrt{(\prod_i g_i^{e_i})} = (\prod_i g_i)$ holds for g_i pairwise non-associated irreducible polynomials.

a) We are in a domain, so $\sqrt{(0)} = (0)$. Polynomials of the form $x - c$ are certainly irreducible, so $(x - c)$ is a maximal ideal, so every element of $\mathcal{J}(\mathbb{C}[x])$ must have all complex numbers among its roots – so it can only be the zero polynomial, because a nonzero polynomial in one variable has only finitely many roots. Hence $\mathcal{J}(\mathbb{C}[x]) = (0)$. Finally, using the irreducible factorisation we determine

$$\begin{aligned} \sqrt{(x-3)^5(x-1)^4(x^3+2)} &= \sqrt{(x-3)^5(x-1)^4(x+\sqrt[3]{2})(x+e^{2\pi i/3}\sqrt[3]{2})(x+e^{4\pi i/3}\sqrt[3]{2})} = \\ &= \left((x-3)(x-1)(x+\sqrt[3]{2})(x+e^{2\pi i/3}\sqrt[3]{2})(x+e^{4\pi i/3}\sqrt[3]{2}) \right) = \\ &= ((x-3)(x-1)(x^3+2)), \\ \sqrt{(x^6-x^4-x^2+1)} &= \sqrt{(x^2-1)(x^4-1)} = \sqrt{(x-1)^2(x+1)^2(x-i)(x+i)} = \\ &= ((x-1)(x+1)(x-i)(x+i)) = (x^4-1). \end{aligned}$$

b) Let $p = \prod_i g_i^{e_i}$ be the factorisation into irreducible polynomials for $p \neq 0$ (for the zero polynomial the statement is verified directly); then we know $\sqrt{(p)} = (\prod_i g_i)$. So it suffices to prove

$$\gcd(p, p') = \prod_i g_i^{e_i-1}.$$

Clearly $\gcd(p, p')$ must divide p , so we know that in the factorisation it is enough to consider the irreducible polynomials g_i and no others; it thus remains to show that each of them occurs with the exponent $e_i - 1$. Let us fix one i and denote $h := \frac{p}{g_i^{e_i}}$. Then by the Leibniz rule

$$p' = (g_i^{e_i}h)' = (g_i^{e_i})'h + g_i^{e_i}h' = e_i g_i^{e_i-1} g_i' h + g_i^{e_i} h' = g_i^{e_i-1} (e_i g_i' h + g_i h').$$

The derivative is therefore divisible by the $(e_i - 1)$ -st power of g_i , but not by the e_i -th, because that would mean $g_i \mid e_i g_i' h + g_i h'$, hence $g_i \mid e_i g_i' h$, which does not hold, because $e_i \neq 0$ is a constant, $g_i \nmid g_i'$ (the nonzero polynomial g_i' has smaller degree than g_i) and h is a product of irreducible polynomials all non-associated with g_i . This completes the proof.

6. Let us work over $K = \mathbb{C}$:

- Prove that $I(V(x^2 - y)) = (x^2 - y)$ and that the algebraic set $V(x^2 - y) \subset \mathbb{C}^2$ is irreducible.
- Determine the set $V(y^4 - x^2, y^4 - x^2 y^2 + x y^2 - x^3) \subset \mathbb{C}^2$ and decompose it into irreducible components.
- * Decompose $V(x^2 + y^2 - 1, x^2 - z^2 - 1) \subset \mathbb{C}^3$ into irreducible components.

Solution. a) Analogously with Problem 1a) one can prove that $V(x^2 - y) = \{(t, t^2) \mid t \in \mathbb{C}\}$. Let us prove that if some polynomial $f \in \mathbb{C}[x, y]$ vanishes on this whole set, then it is a multiple of $x^2 - y$. Consider $\tilde{f} := f(x, x^2) \in \mathbb{C}[x]$. Then $\tilde{f}(t) = f(t, t^2)$, so if $f \in I(V(x^2 - y))$, then $\tilde{f}(t) = 0$. This means that $\tilde{f}$ is a polynomial in one variable which has infinitely many roots, and the only such

polynomial is $\tilde{f} = 0$. Hence we know $f(x, x^2) = 0$, which can be viewed as saying that x^2 is a root of $f \in (\mathbb{C}[x])[y]$, so we can factor out the root binomial $y - x^2$:

$$f = (y - x^2) \cdot f_0 \quad \text{for some } f_0 \in (\mathbb{C}[x])[y] = \mathbb{C}[x, y].$$

This precisely means that $f \in (x^2 - y)$, so we have proved the inclusion $I(V(x^2 - y)) \subseteq (x^2 - y)$. The opposite inclusion is trivial, so we have proved the equality.

Now let us show the irreducibility of $V(x^2 - y)$. For this, let $V(x^2 - y) = A \cup B$ for some algebraic sets A, B , and let us prove that necessarily one of A, B equals $V(x^2 - y)$. We know that $V(x^2 - y) = \{(t, t^2) \mid t \in \mathbb{C}\}$ is an infinite set, so at least one of A, B is infinite; WLOG let it be A . But then necessarily $I(A) \subseteq (x^2 - y)$ by a proof analogous to the previous paragraph: there we could take all complex numbers as the roots t of the polynomial $\tilde{f}$, but it was amply sufficient that *some infinitely many* complex numbers are roots. Every point of A is of the form (t, t^2) and such a t will be a root of $\tilde{f}$ for every $f \in I(A)$, so again we will have $I(A) \subseteq (x^2 - y)$. Applying V to the inclusion $I(A) \subseteq (x^2 - y)$ we obtain

$$V(x^2 - y) \subseteq V(I(A)) = A$$

(we use that V reverses inclusions and that $V(I(A)) = A$ for an algebraic set A), so necessarily $V(x^2 - y) = A$, as we wanted to prove. Hence $V(x^2 - y)$ is irreducible.

b) Here we simply solve the system of polynomial equations

$$\begin{aligned} y^4 - x^2 &= 0, \\ y^4 - x^2 y^2 + x y^2 - x^3 &= 0 \end{aligned}$$

over $\mathbb{C}$. The first equation factorises as $(y^2 - x)(y^2 + x) = 0$, so it suffices to solve the cases $y^2 \mp x = 0$ separately. In these we can use $y^2 = \pm x$ to simplify the second equation to

$$\begin{aligned} (\pm x)^2 - x^2(\pm x) + x(\pm x) - x^3 &= 0, \\ x^2(1 \mp x \pm 1 - x) &= 0, \\ x^2(1 - x)(1 \pm 1) &= 0. \end{aligned}$$

Here we already see that for $\pm = +$ we are solving $2x^2(1 - x) = 0$, which has the (double) root 0 and further the root 1. On the other hand, for $\pm = -$ the whole equation trivialises, which means that every pair (x, y) satisfying $y^2 = -x$ is a solution of the second equation. So from the first case we have finitely many solutions, while from the second one a whole curve of zeros. Altogether:

$$V(y^4 - x^2, y^4 - x^2 y^2 + x y^2 - x^3) = \{(0, 0), (1, 1), (1, -1)\} \cup V(y^2 + x).$$

One-point sets are always algebraic and irreducible, while $V(y^2 + x) = \{(-t^2, t) \mid t \in \mathbb{C}\}$ is irreducible (this can be proved similarly as in part a)), so we have (since $(0, 0) \in V(y^2 + x)$) the irreducible decomposition

$$V(y^4 - x^2, y^4 - x^2 y^2 + x y^2 - x^3) = \{(1, 1)\} \cup \{(1, -1)\} \cup V(y^2 + x)$$

(the point $(0, 0)$ already lies in $V(y^2 + x)$, so it does not give a separate component).

7. If K is a finite field, then every subset of K^n is algebraic.

Solution. One-point sets are algebraic, because

$$\{(a_1, \dots, a_n)\} = V(x_1 - a_1, \dots, x_n - a_n).$$

Further, we know that the union of two algebraic sets is an algebraic set, because $V(IJ) = V(I) \cup V(J)$. By an easy induction it follows that an arbitrary union of finitely many algebraic sets is again an algebraic set. So if we work over a finite field K , then for an arbitrary nonempty $A \subseteq K^n$ we have

$$A = \bigcup_{(a_1, \dots, a_n) \in A} \{(a_1, \dots, a_n)\},$$

which is a finite union of algebraic sets, hence an algebraic set. (The empty set is also algebraic, via $\emptyset = V(1)$.)

8. Observe that for an ideal $I < R$ the radical $\sqrt{I}$ equals $\pi^{-1}(\sqrt{0/I})$, where $\pi : R \rightarrow R/I$ is the natural projection.

Solution. $a^n \in I \iff \pi(a)^n = 0$.

9. Let K be an infinite field and $V = \{(t, t^2, t^3, \dots, t^n) \mid t \in K\} \subset K^n$. Determine $I(V)$ (with a proof!) and, using the problem from the homework (V irreducible $\iff I(V)$ a prime ideal), deduce that V is irreducible.

Solution. (a sketch) We have $I(V) = (x_1^k - x_k \mid k = 2, \dots, n) =: P$, which is a prime ideal, because $K[x_1, \dots, x_n]/P \simeq K[x_1]$ is an integral domain (the isomorphism is $f + P \mapsto f(x_1, x_1^2, \dots, x_1^n)$). Via the equivalence from the homework we thus see that V is an irreducible set.

10. Think through the following characterisations of ideals by means of factor rings: $I < R$ is

- maximal if and only if all nonzero elements of R/I are invertible,
- a prime ideal if and only if a product of nonzero elements in R/I is always nonzero,
- a radical ideal if and only if a power of a nonzero element in R/I is always nonzero.

Solution. The first two bullets only say things we already know: I is maximal if and only if R/I is a field, resp. I is a prime ideal if and only if R/I is an integral domain.

I is a radical ideal if and only if $\sqrt{I} = I$, i.e. when $(\exists n)(a^n \in I) \iff a \in I$. If we reformulate the same in the factor ring, then we want that for an arbitrary $a + I \in R/I$

$$(\exists n)((a + I)^n = 0 + I) \iff a + I = 0 + I.$$

But this says precisely that a power can only be zero when its base was already zero, i.e. that a power of a nonzero element in R/I is already nonzero.

11. Prove that $f(x, y) = y^2 + x^2(x-1)^2 \in \mathbb{R}[x, y]$ is an irreducible polynomial, but the set $V(f) \subset \mathbb{R}^2$ is reducible.

Solution. In $\mathbb{R}$ squares are non-negative, hence for $(a, b) \in \mathbb{R}^2$ we have $f(a, b) = 0$ exactly when $b = 0$ and at the same time $a(a-1) = 0$, so $V(f) = \{(0, 0), (1, 0)\}$, which is clearly a reducible set.

On the other hand f is irreducible: suppose for contradiction that it is not; then it factors as $f = gh$, where both g and h are non-constant. In view of $\deg_y(f) = 2$ we would then have, WLOG, $\deg_y(g) \leq 1$. If we look at f as an element of $\mathbb{R}[x][y]$, then it has leading coefficient one, so $\deg_y(g) = 0$ would mean $g \mid 1$, i.e. g is constant, which is a contradiction.

So we must have $\deg_y(g) = \deg_y(h) = 1$. Moreover f is monic in the sense $f \in \mathbb{R}[x][y]$, so g, h must be monic as well, in other words

$$g = y + g_0, \quad h = y + h_0$$

for some $g_0, h_0 \in \mathbb{R}[x]$. Then comparing the coefficients in

$$y^2 + x^2(x-1)^2 = f = (y + g_0)(y + h_0) = y^2 + (g_0 + h_0)y + g_0h_0$$

already gives $h_0 = -g_0$ and consequently $(x(x-1))^2 = g_0h_0 = -g_0^2$. If now $a \in \mathbb{R}$ is the leading coefficient of g_0 , then taking leading coefficients on both sides we get $1 = -a^2$, which clearly no real number can satisfy.

So altogether f is irreducible, as we wanted.

6.7 Exercises 7

Algebraic number theory

1. Find all units in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ for $D = -2, -3, -7$.

* If you have ever seen Pell's equation, try also $D = 2, 5$.

Solution. It suffices to solve the equation $N(\omega) = \pm 1$ for $\omega \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. For instance for $x + y\frac{1+\sqrt{-3}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ we then solve the equation $x^2 + xy + y^2 = 1$. We rewrite it as $(x + \frac{y}{2})^2 + \frac{3}{4}y^2 = 1$, from which $y^2 \leq \frac{4}{3}$, so $|y| \leq 1$ and we easily finish. It turns out that in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ there are six units: ± 1 and $\frac{\pm 1 \pm \sqrt{-3}}{2}$. For $D = -2$ and $D = -7$ a similar procedure shows that the only units are ± 1 .

For positive D one needs to know the theory around Pell's equation (see the second-year Number Theory course); the units are then (up to sign) the powers of the fundamental unit. For $D = 2$ these will be $\pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$, for $D = 5$ then $\pm\left(\frac{1+\sqrt{5}}{2}\right)^n$, $n \in \mathbb{Z}$, and for instance for $D = 7$ again $\pm(8 + 3\sqrt{7})^n$, $n \in \mathbb{Z}$.

2. Irreducible elements for $K = \mathbb{Q}(\sqrt{-14})$:

- If an element $\alpha \in \mathcal{O}_K$ has norm p , which is a prime in $\mathbb{Z}$, then α is irreducible in $\mathcal{O}_K$.
- Find some irreducible element of $\mathbb{Z}[\sqrt{-14}]$ with prime norm.
- Prove that 3 and $1 + \sqrt{-14}$ are irreducible.
- Prove that $3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$ are two different irreducible factorisations.

Solution. a) Suppose that $\alpha = \beta\gamma$. Then $p = N(\beta)N(\gamma)$ is a factorisation of a prime into a product, so one of $N(\beta)$, $N(\gamma)$ is ± 1 . WLOG let $N(\beta) = \pm 1$. Then β is a unit, so it follows that α cannot be factored into a product of two non-units, i.e. it is an irreducible element.

b) For instance $N(3 + \sqrt{-14}) = 3^2 + 14 = 23$.

c) The norms in K are only non-negative, because $x^2 + 14y^2$ is a positive definite quadratic form. Since $N(3) = 9 = 3^2$, the only way 3 could be reducible would be if it factored into a product of two elements of norm 3. But no such element exists in $\mathcal{O}_K$, because $x^2 + 14y^2 = 3$ has no solution in $\mathbb{Z}$: we estimate $3 \geq 14y^2$, so $|y| < 1$, so $y = 0$, but then $x^2 = 3$ is impossible. Therefore 3 cannot factor nontrivially in $\mathcal{O}_K$.

Similarly $N(1 + \sqrt{-14}) = 15 = 3 \cdot 5$, so for $1 + \sqrt{-14}$ to be reducible it would have to factor into a product of elements of norms 3 and 5. But we already know that elements with norm 3 do not exist in $\mathcal{O}_K$.

d) On the left-hand side we already know that 3 is irreducible. We shall prove that $5 \pm 2\sqrt{-14}$ are irreducible as well. Both have norm $5^2 + 14 \cdot 2^2 = 81 = 3^4$. How could $5 \pm 2\sqrt{-14}$ factor? We want to show that only as an element of norm 1 times an element of norm 81. So it suffices to rule out factorisations with norms $3 \cdot 27$ or $9 \cdot 9$.

A factorisation with norms $3 \cdot 27$ is out of the question, because we already know that elements of norm 3 do not exist. To rule out the second one, we first claim that in $\mathcal{O}_K$ only ± 3 has norm 9. For this let us solve the equation $x^2 + 14y^2 = 9$. Again we estimate $|y| < 1$, so $y = 0$ and we solve $x^2 = 9$, whose only solutions are $x = \pm 3$. So if $5 \pm 2\sqrt{-14}$ were to factor into a product of elements with norms 9, it would up to sign have to be $3 \cdot 3$. But this does not hold; we see that ± 3 does not divide $5 \pm 2\sqrt{-14}$, so we draw the conclusion that $5 \pm 2\sqrt{-14}$ is irreducible.

This verifies that 81 has in $\mathcal{O}_K$ two different factorisations into products of irreducible elements, so it is certainly not a Gaussian domain.

3. Principal ideals for $K = \mathbb{Q}(\sqrt{-14})$:

- Prove that $(17 + 2\sqrt{-14}, 20 + \sqrt{-14}) = (3 - \sqrt{-14})$ is a principal ideal in $\mathbb{Z}[\sqrt{-14}]$.
- $(2, \sqrt{-14})$ is not a principal ideal in $\mathbb{Z}[\sqrt{-14}]$.
- Prove that $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14})$ and that this is a proper ideal which is not principal.

Solution. a) We prove the equality of ideals as two inclusions. One is easy:

$$3 - \sqrt{-14} = (20 + \sqrt{-14}) - (17 + 2\sqrt{-14}),$$

so $(3 - \sqrt{-14}) \subseteq (17 + 2\sqrt{-14}, 20 + \sqrt{-14})$. For the second inclusion we want to show that both $17 + 2\sqrt{-14}$ and $20 + \sqrt{-14}$ are multiples of $3 - \sqrt{-14}$. We do not need to know exactly which multiples they are, so let us just look in the factor ring $\mathcal{O}_K/(3 - \sqrt{-14})$. There $\sqrt{-14} \equiv 3$, so together with $3 - \sqrt{-14} \mid N(3 - \sqrt{-14}) = 23$ we obtain

$$17 + 2\sqrt{-14} \equiv 17 + 2 \cdot 3 = 23 \equiv 0, \quad 20 + \sqrt{-14} \equiv 20 + 3 = 23 \equiv 0,$$

so indeed $17 + 2\sqrt{-14}, 20 + \sqrt{-14} \in (3 - \sqrt{-14})$, hence $(17 + 2\sqrt{-14}, 20 + \sqrt{-14}) \subseteq (3 - \sqrt{-14})$.

b) Suppose for contradiction that $(2, \sqrt{-14}) = (\alpha)$. Then $N(\alpha)$ must be a common divisor of $N(2) = 4$ and $N(\sqrt{-14}) = 14$, so $N(\alpha) \mid 2$. Similarly as in the previous problem we easily show that elements with norm 2 do not exist, so the only remaining possibility is $N(\alpha) = 1$. Then $\alpha \mid 1$, so we may WLOG take $\alpha = 1$.

So we would have to have $(2, \sqrt{-14}) = \mathcal{O}_K$. But a general element of the ideal $(2, \sqrt{-14})$ is some

$$(a + b\sqrt{-14}) \cdot 2 + (c + d\sqrt{-14}) \cdot \sqrt{-14} = (2a - 14d) + (2b + c)\sqrt{-14},$$

which always has an even rational part, so e.g. 1 cannot be expressed in this way, which contradicts $(2, \sqrt{-14}) = \mathcal{O}_K$. So $(2, \sqrt{-14})$ must be non-principal.

c) First let us verify the equality of ideals, again as two inclusions. Successively we have

$$\begin{aligned} 2 + \sqrt{-14} &= 3 - (1 - \sqrt{-14}) \in (3, 1 - \sqrt{-14}), \\ 7 + 2\sqrt{-14} &= 2(2 + \sqrt{-14}) + 3 \in (3, 1 - \sqrt{-14}), \end{aligned}$$

so $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) \subseteq (3, 1 - \sqrt{-14})$. From the opposite side then

$$\begin{aligned} 3 &= (7 + 2\sqrt{-14}) - 2(2 + \sqrt{-14}) \in (2 + \sqrt{-14}, 7 + 2\sqrt{-14}), \\ 1 - \sqrt{-14} &= 3 - (2 + \sqrt{-14}) \in (2 + \sqrt{-14}, 7 + 2\sqrt{-14}), \end{aligned}$$

so $(3, 1 - \sqrt{-14}) \subseteq (2 + \sqrt{-14}, 7 + 2\sqrt{-14})$.

Further, suppose for contradiction that $(3, 1 - \sqrt{-14}) = (\alpha)$. Then $N(\alpha) \mid \gcd(N(3), N(1 - \sqrt{-14})) = \gcd(9, 15) = 3$. Since elements of norm 3 do not exist, this would mean $N(\alpha) = 1$, so $(3, 1 - \sqrt{-14}) = \mathcal{O}_K$. We shall contradict this by observing that all elements of $(3, 1 - \sqrt{-14})$ have norm divisible by three. For this let us consider $3\beta + (1 - \sqrt{-14})\gamma$; then computing in the factor ring $\mathcal{O}_K/(3)$ we have

$$\begin{aligned} N(3\beta + (1 - \sqrt{-14})\gamma) &= (3\beta + (1 - \sqrt{-14})\gamma)(3\beta' + (1 + \sqrt{-14})\gamma') \equiv \\ &\equiv (1 - \sqrt{-14})\gamma(1 + \sqrt{-14})\gamma' = N(1 - \sqrt{-14})N(\gamma) = 15N(\gamma) \equiv 0 \pmod{3}. \end{aligned}$$

This already means that e.g. $1 \notin (3, 1 - \sqrt{-14})$, so we have a contradiction and this ideal could not have been principal.

4. Multiplication of ideals for $K = \mathbb{Q}(\sqrt{-14})$:

- $(5 + \sqrt{-14}, 2 + \sqrt{-14})(4 + \sqrt{-14}, 2 - \sqrt{-14}) = (6, 3\sqrt{-14})$.
- Let $I = (3, 1 + \sqrt{-14})$. Then $II' = (3)$, I is not principal and $I \neq I'$.
- Let $J = (5, 1 + \sqrt{-14})$. Then $(15) = IJJ'$. Use this to find two different irreducible factorizations of 15.
- * I, J are prime ideals.

Solution. a) Before multiplying we choose a nicer set of generators for the ideals:

$$(5 + \sqrt{-14}, 2 + \sqrt{-14}) = (3, 2 + \sqrt{-14}), \quad (4 + \sqrt{-14}, 2 - \sqrt{-14}) = (6, 2 - \sqrt{-14}).$$

Then we multiply out the generators with each other, which gives the result written by means of four generators:

$$(3, 2 + \sqrt{-14})(6, 2 - \sqrt{-14}) = (18, 6 - 3\sqrt{-14}, 12 + 6\sqrt{-14}, 18).$$

Now we simplify this expression. The duplicate 18 can be omitted, and further 3 can be factored out, so

$$(18, 6 - 3\sqrt{-14}, 12 + 6\sqrt{-14}, 18) = 3 \cdot (6, 2 - \sqrt{-14}, 4 + 2\sqrt{-14}).$$

Here we now rewrite $(2 - \sqrt{-14}, 4 + 2\sqrt{-14}) = (2 - \sqrt{-14}, 8)$, so

$$3 \cdot (6, 2 - \sqrt{-14}, 4 + 2\sqrt{-14}) = 3 \cdot (6, 8, 2 - \sqrt{-14}).$$

Already in $\mathbb{Z}$ we have $(6, 8) = (2)$, so all the more in $\mathcal{O}_K$, and we finally rewrite

$$3 \cdot (6, 8, 2 - \sqrt{-14}) = 3 \cdot (2, 2 - \sqrt{-14}) = 3 \cdot (2, \sqrt{-14}) = (6, 3\sqrt{-14}).$$

b) By Proposition 4.11 we have $II' = (N(3), \text{Tr}(3 \cdot (1 - \sqrt{-14})), N(1 + \sqrt{-14})) = (9, 6, 15)$. This is an ideal generated by integers, so the result will be generated by their gcd in the sense of $\mathbb{Z}$, hence $II' = (3)$. The ideal $I' = (3, 1 - \sqrt{-14})$ we have already seen in **3.c**), from where we know that it is not principal, so I cannot be principal either (if $I = (\alpha)$, then $I' = (\alpha')$).

Finally, let us assume for contradiction that $I = I'$. Then $I = (3, 1 + \sqrt{-14}, 1 - \sqrt{-14})$. But then

$$1 = 3 - (1 + \sqrt{-14}) - (1 - \sqrt{-14}) \in I,$$

so $I = \mathcal{O}_K$, which contradicts $NI = 3$.

c) Let us show $NJ = 5$. We compute this using $JJ' = (N(5), \text{Tr}(5 \cdot (1 - \sqrt{-14})), N(1 + \sqrt{-14})) = (25, 10, 15)$, which we again compute via the gcd in $\mathbb{Z}$ as (5) . With this we now rewrite

$$IJJ'J' = (II')(JJ') = (3)(5) = (15).$$

One irreducible factorisation of 15 is $3 \cdot 5$. About 3 we already know that it is irreducible, and for 5 we prove it analogously: if it factored nontrivially, it would have to be into a product of elements of norm 5, but such elements do not exist, because $x^2 + 14y^2 = 5$ has no solution.

For the second factorisation let us show that $IJ = (1 + \sqrt{-14})$. We write out the ideal on the left as

$$IJ = (3, 1 + \sqrt{-14})(5, 1 + \sqrt{-14}) = (15, 3 + 3\sqrt{-14}, 5 + 5\sqrt{-14}, (1 + \sqrt{-14})^2).$$

Since $N(1 + \sqrt{-14}) = 15$, all four of these generators are multiples of $1 + \sqrt{-14}$, so certainly $(1 + \sqrt{-14}) \mid IJ$. If equality did not occur in this divisibility, we would have to have $N(IJ) > N((1 + \sqrt{-14}))$. But both these norms are equal to 15, so equality must already have occurred.

(Alternatively, it suffices to realise that from $3 \cdot (1 + \sqrt{-14})$ and $5 \cdot (1 + \sqrt{-14})$ one can already combine $1 \cdot (1 + \sqrt{-14})$.)

d) Let us observe more generally that an ideal with prime norm $NI = p$ must be a prime ideal (the converse does not hold, however – there exist prime ideals whose norm is not a prime!). Since $NI = 3$ and $NJ = 5$, this covers both our ideals.

Consider the factorisation of I into primes, say $I = P_1 \cdots P_k$. The norm is multiplicative, so then $p = NI = NP_1 \cdots NP_k$. Prime ideals are always proper ideals, so we always have $NP_i > 1$. But then

only one factor can occur in the product, otherwise we would factor a prime nontrivially. So $k = 1$ and $I = P_1$ is a prime ideal.

5. Let G be a subgroup of the additive group $\mathbb{Z}^n$, where $n \in \mathbb{N}$. Prove that $G \simeq \mathbb{Z}^m$ for some m , $0 \leq m \leq n$. As a consequence, observe that an arbitrary ideal in $\mathcal{O}_K$ can be written with at most two generators.

Solution. First, let G , considered as a set of vectors of the $\mathbb{Q}$ -vector space $\mathbb{Q}^n$, generate some subspace V , and let this space be m -dimensional. We show that then $G \simeq \mathbb{Z}^m$.

Let us proceed by induction on m . For $m = 0$ the statement is obvious, because $G = 0$. For $m = 1$ the group G generates only a line, so we can choose on this line the shortest nonzero vector b . Every other element $g \in G$ must be an integer multiple of b , because otherwise $g - k \cdot b$ for some suitable k would be shorter than b .

Now let $m \geq 2$. From the generating set G of the vector space V let us choose some basis $c_1, \dots, c_m$. Let then V' be the linear span of $c_1, \dots, c_{m-1}$ and subsequently $G' := G \cap V'$. Certainly $c_1, \dots, c_{m-1} \in G'$, so G' generates V' , and by the induction hypothesis $G' \simeq \mathbb{Z}^{m-1}$, which means that G' is a free abelian group with some basis $b_1, \dots, b_{m-1}$. It then remains only to choose a suitable $b_m \in G$ so that $b_1, \dots, b_m$ is a basis of G as a free abelian group.

With the standard scalar product restricted from $\mathbb{Q}^n$, the space V' must have a one-dimensional orthogonal complement inside V – let it be generated by some vector x . WLOG let us multiply it by a common multiple of the denominators occurring in its coordinates, so that then $x \in \mathbb{Z}^n$. Since x is a normal vector to V' , the distance of any vector from V' is directly proportional to its scalar product with x . So let us choose some element $b_m \in G \setminus G'$ minimising $|x \cdot b_m|$. This is certainly possible, because all the values $x \cdot b_m$ are integers.

Let us prove that the set $b_1, \dots, b_{m-1}, b_m$ now generates G . Since it is at the same time a $\mathbb{Q}$ -linearly independent set, it will then automatically be a basis of G as a free abelian group. Consider an arbitrary $g \in G$. Because $b_1, \dots, b_m$ is certainly at least a basis of V , we can express

$$g = q_1 b_1 + \dots + q_m b_m$$

for uniquely determined $q_1, \dots, q_m \in \mathbb{Q}$. We want to prove that these are in fact integers. First suppose for contradiction that $q_m \notin \mathbb{Z}$. Then we can consider

$$\tilde{g} := g - \lfloor q_m \rfloor b_m \in G \setminus G',$$

which then gives $|x \cdot \tilde{g}| = (q_m - \lfloor q_m \rfloor) |x \cdot b_m| < |x \cdot b_m|$, contradicting the choice of b_m . So we have $q_m \in \mathbb{Z}$. Consequently $g - q_m b_m$ lies in G , but at the same time in V' , hence it lies in G' , and so it must have integer coordinates with respect to $b_1, \dots, b_{m-1}$, so $q_1, \dots, q_{m-1} \in \mathbb{Z}$. Altogether we have thus proved that G is a free abelian group with basis $b_1, \dots, b_m$.

6. Let $K = \mathbb{Q}(\sqrt{D})$ and $\omega = \sqrt{D}$, resp. $\frac{1+\sqrt{D}}{2}$ for $D \equiv 2, 3$, resp. $1 \pmod{4}$. For $m \in \mathbb{Z}$ and $\alpha = a + b\omega \in \mathcal{O}_K$ prove that $m \mid \alpha$ in $\mathcal{O}_K$ if and only if $m \mid a, b$ in $\mathbb{Z}$. Observe that for $D \equiv 1 \pmod{4}$ the same need not hold for $m \mid a + b\sqrt{D}$, $a, b \in \mathbb{Z}$.

Solution. By Theorem 4.3 we know that $\mathcal{O}_K = \mathbb{Z}[\omega]$. Since ω is an integral element over $\mathbb{Z}$ and has a quadratic minimal polynomial, we know that $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$ in the sense of abelian groups, i.e. that $\mathcal{O}_K$ is a free abelian group with free basis $1, \omega$. In other words, $a + b\omega$ for $a, b \in \mathbb{Q}$ is an element of $\mathcal{O}_K$ if and only if $a, b \in \mathbb{Z}$. From this (for $m \neq 0$)

$$m \mid a + b\omega \iff \frac{a}{m} + \frac{b}{m}\omega \in \mathcal{O}_K \iff \frac{a}{m}, \frac{b}{m} \in \mathbb{Z} \iff m \mid a, b.$$

For $m = 0$ it suffices to argue

$$0 \mid a + b\omega \iff a + b\omega = 0 \iff a = b = 0,$$

because $1, \omega$ is a $\mathbb{Q}$ -linear basis of K .

For $D \equiv 1 \pmod{4}$ the same no longer necessarily holds with $\sqrt{D}$ in place of ω , because e.g. $2 \mid 1 + \sqrt{D}$ in $\mathcal{O}_K$, since $\frac{1+\sqrt{D}}{2} = \omega \in \mathcal{O}_K$, and yet $2 \nmid 1$.

7. Solve the Diophantine equations $x^2 + 1 = y^5$, $x^2 + 3 = y^3$ and $x^2 + 4 = y^3$.

Solution. As a model example let us solve $x^2 + 1 = y^5$; we claim that the only solution is $(x, y) = (0, 1)$. We factor the left-hand side in $\mathbb{Z}[i]$ as $(x+i)(x-i) = y^5$. Since $\mathbb{Z}[i]$ is a Gaussian domain (in fact even a PID, $\mathbb{Q}(i)$ has class number 1), we make use of unique factorisation: if we show that the brackets on the left-hand side are coprime, then each of them must already be a fifth power on its own, possibly up to multiplication by a unit.

Let d be some common divisor of $x+i$ and $x-i$. Then we must also have $d \mid (x+i) - (x-i) = 2i$, so $N(d) \mid N(2i) = 4$. We want to show that the only possibility is $N(d) = 1$, whereupon d is a unit, so that $x+i, x-i$ are coprime. So suppose for contradiction that $N(d) \neq 1$; then necessarily $2 \mid N(d)$. That means $2 \mid N(x+i) = x^2 + 1 = y^5$, so y is even. Then x is odd, so modulo 4 we get

$$2 \equiv x^2 + 1 \equiv y^5 \equiv 0 \pmod{4},$$

which is a contradiction. So $x+i, x-i$ really are coprime.

Then $x+i$ is a fifth power times a unit, i.e. $x+i = u\alpha^5$ for some $\alpha \in \mathbb{Z}[i]$ and some $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Since $\mathbb{Z}[i]^\times$ is a four-element (indeed cyclic) group, we have $u = u^5$, so we can simplify to $x+i = (u\alpha)^5$. If we then denote $u\alpha = a+bi$, $a, b \in \mathbb{Z}$, we can write out

$$x+i = (a+bi)^5 = (a^5 - 10a^3b^2 + 5ab^4) + (5a^4b - 10a^2b^3 + b^5)i.$$

Comparing the imaginary parts we then have the equation

$$1 = 5a^4b - 10a^2b^3 + b^5 = b(5a^4 - 10a^2b^2 + b^4).$$

From this $b \mid 1$, so $b = \pm 1$. For $b = -1$ we get

$$-1 = 5a^4 - 10a^2 + 1,$$

which cannot hold modulo 5. For $b = 1$ we get

$$1 = 5a^4 - 10a^2 + 1,$$

which simplifies to $a^2(a^2 - 2) = 0$. For integer a the expression $a^2 - 2$ will always be nonzero, so the only solution is $a = 0$. Altogether we have thus obtained that we must have $a+bi = i$, from which we compute

$$x+i = (a+bi)^5 = i^5 = i,$$

so $x = 0$ and consequently $y = 1$.

8. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$, resp. $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ for $D \equiv 2, 3$, resp. $1 \pmod{4}$.

Solution. Let $K = \mathbb{Q}(\sqrt{D})$, where D is a squarefree integer. An element $\alpha \in K$ is integral over $\mathbb{Z}$ if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients. Let us first set aside the rational α : by the rational root theorem, $\alpha \in \mathbb{Q}$ is integral over $\mathbb{Z}$ only when $\alpha \in \mathbb{Z}$. So further let us consider $\alpha \in K \setminus \mathbb{Q}$. Such an α has the minimal polynomial

$$(x - \alpha)(x - \alpha') = x^2 - x(\alpha + \alpha') + \alpha\alpha' = x^2 - x \operatorname{Tr}(\alpha) + N(\alpha).$$

So α will be integral if and only if both $\operatorname{Tr}(\alpha)$ and $N(\alpha)$ are integers. (Careful, this is specific to quadratic number fields; in fields of higher degree integrality of the norm and the trace is in general not enough...)

So let us have $\alpha = a + b\sqrt{D}$. First, thanks to $\mathbb{Z} \ni \text{Tr}(\alpha) = 2a$, the number a must be an integer or a half of an odd number. First let $a \in \mathbb{Z}$. Then thanks to $\mathbb{Z} \ni N(\alpha) = a^2 - Db^2$ we must also have $Db^2 \in \mathbb{Z}$. By means of p -valuations this means the same as $v_p(Db^2) \geq 0$ for every p , where we write out the valuation on the left-hand side as $v_p(D) + 2v_p(b)$. We assume that D is a squarefree integer, so $v_p(D)$ can only be 0 or 1. In any case then

$$v_p(b) \geq -\frac{1}{2}v_p(D) \geq -\frac{1}{2},$$

so $v_p(b) \geq 0$, hence b is an integer. In this case we have thus arrived at $\alpha \in \mathbb{Z}[\sqrt{D}]$, whose elements are always integral for an arbitrary D (e.g. because $\sqrt{D}$ is integral and $\mathcal{O}_K$ is a ring).

Now let us consider the case when $a = \ell/2$ for some odd ℓ . We show that this can occur only for $D \equiv 1 \pmod{4}$ and that it then forces $b = m/2$, where m is odd. This will thus correspond to $\alpha \in \mathbb{Z} \left[\frac{1+\sqrt{D}}{2} \right]$. Let $m := 2b$; then we have $2\alpha = \ell + m\sqrt{D}$. If α was integral, 2α must be integral as well, and since ℓ is an integer, we derive $m \in \mathbb{Z}$ just as in the previous paragraph. So it remains to show that m must be odd and D must be $1 \pmod{4}$. For this let us compute modulo 4: since $N(2\alpha) = 4N(\alpha)$ and $N(\alpha)$ was an integer, we have

$$0 \equiv N(\ell + m\sqrt{D}) = \ell^2 - Dm^2 \equiv 1 - Dm^2 \pmod{4}.$$

For even m we would have $m^2 \equiv 0$, which gives a contradiction in the previous congruence, so m certainly must be odd. Then $m^2 \equiv 1$, so we obtain $1 - D \equiv 0$, hence $D \equiv 1 \pmod{4}$.

Subsequently we only verify that all the elements of $\mathbb{Z} \left[\frac{1+\sqrt{D}}{2} \right]$ are for $D \equiv 1 \pmod{4}$ really integral. For this it suffices to verify that $\frac{1+\sqrt{D}}{2}$ itself is integral, which however follows from the fact that it has trace $1 \in \mathbb{Z}$ and norm $\frac{1-D}{4} \in \mathbb{Z}$.

9. Let $K = \mathbb{Q}(\sqrt{D})$. If $P < \mathcal{O}_K$ is a nonzero prime ideal and $\alpha \in \mathcal{O}_K$, then $\alpha^{NP} \equiv \alpha \pmod{P}$.

Solution. It suffices to know that the factor ring $\mathcal{O}_K/P$ has exactly NP elements. If $\alpha \equiv 0 \pmod{P}$, then the conclusion is obvious. Otherwise α is nonzero in the finite field $\mathcal{O}_K/P$. So it lies in its multiplicative group, which has $NP - 1$ elements, so by Lagrange's theorem from group theory we have $\alpha^{NP-1} \equiv 1 \pmod{P}$. Multiplying this congruence by α then gives the desired conclusion.

10. Let R be a Gaussian domain and T its field of fractions. If $u \in T$ is integral over R , then $u \in R$.

Solution. It suffices to show $v_p(u) \geq 0$ for all prime elements p . So suppose for contradiction that $v := v_p(u) < 0$ for some p . Let u be a root of a monic polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, where $c_i \in R$. Then

$$u^n + c_{n-1}u^{n-1} + \cdots + c_1u + c_0 = 0.$$

Since $c_i \in R$, we have $v_p(c_i) \geq 0$. On the left-hand side u^n has valuation $n \cdot v$, while every other term $c_i u^i$ has valuation $i \cdot v + v_p(c_i) \geq iv$. Since $v < 0$, we have $iv > nv$, so u^n has strictly lower valuation than all the other terms on the left-hand side. Consequently the whole left-hand side will have valuation nv . But that means $nv = v_p(0) = \infty$, which is a contradiction.

11. * A prime $p > 5$ is given together with a natural number k such that $p \mid k^2 + 5$. Prove that there exist natural numbers m, n satisfying $p^2 = m^2 + 5n^2$. Assume that you know that the class group of $\mathbb{Z}[\sqrt{-5}]$ has two elements.

Solution. Denote $K = \mathbb{Q}(\sqrt{-5})$; then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The given condition says that k is a root of $x^2 + 5$ over $\mathbb{F}_p$, so by Theorem 4.20 the ideal (p) factors in $\mathcal{O}_K$ as a product of two prime ideals PP' . Let us check that these are two different prime ideals: since $p \nmid 5$, we cannot have $k \equiv 0 \pmod{p}$, so k is not a root of the derivative $(x^2 + 5)' = 2x$ (we have $p > 5$, so also $p \nmid 2$), so it is not a double root of $x^2 + 5$.

So now $N(P) = p$. The ideal P itself may or may not be principal. But since the class group has two elements, the square of any ideal must be trivial in the class group, i.e. the square of any ideal is a principal ideal. So we may take $P^2 = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. Since $P \neq P'$, we have $(p) = PP' \nmid P^2 = (\alpha)$, so if we write $\alpha =: x + y\sqrt{-5}$, then p does not divide at least one of x, y . We have

$$p^2 = N(P)^2 = N(P^2) = N(\alpha) = x^2 + 5y^2.$$

So if p divided one of x, y , it would have to divide the other one as well. So $p \nmid x, y$; in particular both x and y are then nonzero. Taking $m := |x|$, $n := |y|$ solves the problem.

12. ** Try to think through that when $D \equiv 1 \pmod{4}$, then $\mathbb{Z}[\sqrt{D}]$ can never be a Gaussian domain.

Solution. For $D \equiv 1 \pmod{4}$ we know that $\frac{1+\sqrt{D}}{2} \in \mathbb{Q}(\sqrt{D})$ is integral over $\mathbb{Z}$, but does not lie in $\mathbb{Z}[\sqrt{D}]$. At the same time $\mathbb{Q}(\sqrt{D})$ is the field of fractions of $\mathbb{Z}[\sqrt{D}]$, so by Problem 10. the ring $\mathbb{Z}[\sqrt{D}]$ cannot be Gaussian.

7. Homework assignments

In the version from the winter semester 2023/2024.

7.1 Homework 1

1. Consider a ring R . Prove that R is an integral domain if and only if $R[x]$ is an integral domain.
2. Let R be a ring. Prove that if $R[x]$ is Noetherian, then R is Noetherian as well.
3. Let R be a Gaussian domain and consider polynomials $f, g \in R[x]$ which are coprime in this ring. Prove that the ideal $(f, g) < R[x]$ contains some nonzero element of R .
4. Let R be a ring and $I, J < R$ comaximal ideals. Prove that for arbitrary natural numbers m, n the ideals I^m, J^n are comaximal.
5. By a *multiplicative set* in a ring R we mean a set $S \subset R$ which is nonempty, does not contain 0 and is closed under multiplication. Using Zorn's lemma (without using Lemma 1.24 of the notes) prove: if $S \subset R$ is a multiplicative set and an ideal $I < R$ satisfies $I \cap S = \emptyset$, then there exists a prime ideal $P \supset I$ satisfying $P \cap S = \emptyset$.

7.2 Homework 2

1. Find $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\sqrt{2}, \sqrt{7}) = \mathbb{Q}(\alpha)$. (Please prove carefully, do not rely on “obvious” statements which are not obvious.)
2. Let U be a field and $G < \text{Aut}(U)$. Prove that then for all $\varphi \in \text{Aut}(U)$ we have $\text{Fix}(U, \varphi G \varphi^{-1}) = \varphi(\text{Fix}(U, G))$.
3. Let T be the splitting field of the polynomial $x^4 - 5$ over $\mathbb{Q}$. Determine the degree of the extension $[T : \mathbb{Q}]$.
4. For all the possible root fields U of the polynomial $x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}$ describe $\text{Gal}(U/\mathbb{Q})$ and find some “known” group it is isomorphic to.

7.3 Homework 3

1. Let V be the splitting field of the polynomial $f(x) = x^4 - 2$ over the field $\mathbb{Q}$. Decide whether $V \supset \mathbb{Q}$ is a Galois extension and determine $\text{Gal}(V/\mathbb{Q})$. Find all the fields T such that $V \supset T \supset \mathbb{Q}$, $[V : T] = 2$ and at the same time $T \supset \mathbb{Q}$ is a normal extension.
2. Let P be a prime ideal in a ring R and I, J proper ideals in R . Prove:
 - a) $\sqrt{I} \subseteq P$ if and only if $I \subseteq P$.
 - b) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

3. Let K be a field and $V \subset K^n$ a nonempty algebraic set. Prove that V is irreducible if and only if $I(V)$ is a prime ideal.
4. Let $R \subset S \subset T$ be domains. Prove:
- a) If T is a finitely generated S -module and S a finitely generated R -module, then T is also a finitely generated R -module.
 - b) Let $\alpha, \beta \in S$. If α is an element integral over R and β an element integral over $R[\alpha]$, then β is also an element integral over R .
 - c) $\sqrt{3\sqrt[4]{5} + 6\sqrt[7]{8}}$ is an element integral over $\mathbb{Z}$.