**Compact course notes**

# Pure Math 345, Fall 2012

*Polynomials, Rings, and Finite Fields*

Professor: K. Hare
transcribed by: J. Lazovskis
University of Waterloo
December 19, 2012

## Contents

# 1 Rings and fields

## 1.1 Definitions

**Definition 1.1.1.** A ring is a set $R$ with two binary operations $+$ and $\cdot$ that satisfy for all $a, b, c \in R$ the following rules:

A1. $a + b \in R$
A2. $(a + b) + c = a + (b + c)$
A3. $a + b = b + a$
A4. $\exists$ 0 such that $a + 0 = 0 + a = a$
A5. $\forall\ a\ \exists\ d$ such that $a + d = 0$

M1. $a \cdot b \in R$
M2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

AM. $a \cdot (b + c) = a \cdot b + a \cdot c$
$(a + b) \cdot c = a \cdot c + b \cdot c$

Given an element $a \in R$, the $d$ in A5 is also termed $-a$.

**Remark 1.1.2.** If a ring has the M3 property, then it is a commutative ring.
If a ring has the M4 property, then it is a ring with unity.
If a ring has the M5 property, then it is a division ring.

**Example 1.1.3.** These are some common examples of different types of rings.

| | |
|---|---|
| $\mathbb{Z}$ | commutative ring with unity, not a division ring |
| $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ | commutative division ring with unity |
| $2\mathbb{Z}$ | Commutative ring, no unity, not a division ring |
| $M(2, \mathbb{R})$ | non-commutative ring with unity |
| $R_1 \times R_2$ | commutative ring for $R_1, R_2$ commutative rings |

**Remark 1.1.4.** Let $n \in \mathbb{N}$ and $a \in R$. Then let $n \cdot a := \underbrace{a + a + \cdots + a}_{n \text{ times}}$ and $a^n := \underbrace{a \cdot a \cdots a}_{n \text{ times}}$

## 1.2 Properties

**Proposition 1.2.1.** Let $-a, -b$ be additive inverses of $a, b \in R$. Let 0 be the additive identity. Then
**1.** $0 \cdot a = a \cdot 0 = 0$
**2.** $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$
**3.** $(-a) \cdot (-b) = a \cdot b$

*Proof:*

**1.**
$$\begin{aligned} 0 \cdot a &= 0 \cdot a + 0 \\ &= 0 \cdot a + 0 \cdot a + (-(0 \cdot a)) \\ &= (0 + 0) \cdot a + (-(0 \cdot a)) \\ &= 0 \cdot a + (-(0 \cdot a)) \\ &= 0 \end{aligned}$$

**2.**
$$\begin{aligned} (-a) \cdot b &= (-a) \cdot b + a \cdot b + (-(a \cdot b)) \\ &= (-a + a) \cdot b + (-(a \cdot b)) \\ &= 0 \cdot b + (-(a \cdot b)) \\ &= 0 + (-(a \cdot b)) \\ &= -(a \cdot b) \\ &= 0 + (-(a \cdot b)) \\ &= a \cdot 0 + (-(a \cdot b)) \\ &= a \cdot (-b + b) + (-(a \cdot b)) \\ &= a \cdot (-b) + a \cdot b + (-(a \cdot b)) \\ &= a \cdot (-b) + 0 \\ &= a \cdot (-b) \end{aligned}$$

**3.**
$$\begin{aligned} (-a) \cdot (-b) &= (-a) \cdot (-b) + 0 \\ &= (-a) \cdot (-b) + (-(a \cdot b)) + a \cdot b \\ &= (-a) \cdot (-b) + (-a) \cdot b + a \cdot b \\ &= (-a) \cdot (-b + b) + a \cdot b \\ &= (-a) \cdot 0 + a \cdot b \\ &= 0 + a \cdot b \\ &= a \cdot b \end{aligned}$$

■

**Definition 1.2.2.** Let $R_1$ be a ring. If $R_2 \subset R_1$ is also a ring under the same binary operations as $R_1$, then $R_2$ is termed a subring of $R_1$, and the relation is given by $R_2 \ll R_1$.

**Example 1.2.3.** These are some examples of subrings.

1. $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$ is a commutative subring of $M(2, \mathbb{R})$
2. Any subring of a commutative ring is commutative
3. $\underbrace{2\mathbb{Z} \ll \mathbb{Z} \ll \underbrace{\mathbb{Q} \ll \mathbb{R} \ll \mathbb{C}}_{\text{division rings}}}_{\text{rings with unity}}$

## 1.3 Integral domains

**Example 1.3.1.** Consider the multiplication tables for the rings $\mathbb{Z}_4$ and $\mathbb{Z}_5$.

| $\cdot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

| $\cdot$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

We may observe the following:

· As both tables are symmetric along the diagonal, both $\mathbb{Z}_4$ and $\mathbb{Z}_5$ are commutative.
· By the second row/column of each, we see that both have unity.
· Since there is no 1 in the row/column of 2 in $\mathbb{Z}_4$, we see that $\mathbb{Z}_4$ is not a division ring.
· Since every row/column of $\mathbb{Z}_5$ has a 1, it means that $\mathbb{Z}_5$ is a division ring.
· Interestingly, $2 \cdot 2 = 0$ in $\mathbb{Z}_4$.

**Definition 1.3.2.** Let $a, b \in R$ non-zero such that $a \cdot b = 0$. Then $a$ and $b$ are termed zero divisors.

**Theorem 1.3.3.** Let $a \in \mathbb{Z}_n$ be non-zero. Then $a$ is a zero divisor if and only if $\gcd(a, n) > 1$.

*Proof:* ($\Leftarrow$) Let $\gcd(a, n) = b > 1$. Then there exist some $a', n'$ such that $a = b \cdot a'$ and $n = b \cdot n'$, so $n' < n$. Then $a \cdot n' = a' \cdot b \cdot n' = a' \cdot n = a' \cdot 0 = 0$, proving that $a$ is a zero divisor.

($\Rightarrow$) Let $\gcd(a, n) = 1$. Then by the EEA, there exist some $c, d$ such that $a \cdot c + d \cdot n = 1$. This tells us that $a \cdot c \equiv 1 \pmod{n}$. Now suppose there exists a zero divisor $e$ such that $a \cdot e = 0$, so then we have both

$$(c \cdot a) \cdot e = 1 \cdot e = e$$
$$(c \cdot a) \cdot e = c \cdot (a \cdot e) = c \cdot 0 = 0$$

Since $e$ must be non-zero as it is a zero divisor, this is a contradiction. Therefore the assumption that there exists a zero divisor $e$ such that $a \cdot e = 0$ was false, so there is no zero divisor. ■

**Theorem 1.3.4.** Let $a, b, c \in R$ and suppose that $a \cdot b = a \cdot c$ with $a$ not a zero divisor of $R$. Then $b = c$.

*Proof:* First note $ab = ac \implies ab - ac = 0 \implies a(b - c) = 0$. Since $a$ is not a zero divisor, $c - b = 0$, so $c = b$. ■

**Definition 1.3.5.** A ring $R$ is termed an integral domain if the following two conditions are satisfied:

1. $R$ is a commutative ring with unity
2. $R$ has no zero divisors

**Example 1.3.6.** These are some examples of integral domains:

1. $\mathbb{Z}_p$ for $p$ prime
2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$
3. $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3, i^2 = -1\}$

Note that $R_1 \times R_2$ for $R_1, R_2$ integral domains is not an integral domain.

**Definition 1.3.7.** Let $R_1 \subset R_2$ both be integral domains. Then $R_1$ is termed a subdomain of $R_2$.

For example, $\mathbb{Z}$ is a subdomain of $\mathbb{Q}$ is a subdomain of $\mathbb{R}$ is a subdomain of $\mathbb{C}$.

**Definition 1.3.8.** Let $R$ be a ring with unity. Then $a$ is a unit if there exists $b \in R$ such that $a \cdot b = 1$.

**Remark 1.3.9.** If $a, b \in R$ are units, then $a \cdot b$ is a unit.

**Example 1.3.10.** These are some examples of rings with unity and their respective units.

1. $\mathbb{Z}$ : $1, -1$
2. $\mathbb{Q}$ : $\mathbb{Q} \setminus \{0\}$
3. $\mathbb{Z}_8$ : $1, 3, 5, 7$
4. $M(2, \mathbb{R})$ : the set of invertible matrices
5. Any division ring: all non-zero elements

## 1.4 Fields

**Definition 1.4.1.** Let $R$ be a commutative ring with unity such that every non-zero element is a unit. Then $R$ is termed a field.

**Remark 1.4.2.** The following relation exists among different ring types:

$$\text{Fields} \subsetneq \text{Division rings} \subsetneq \text{Rings with unity} \subsetneq \text{Rings}$$

**Example 1.4.3.** There exist non-commutative division rings, such as

$$\mathbb{H} = \left\{ \begin{bmatrix} u & v \\ -\bar{u} & \bar{v} \end{bmatrix} \,\middle|\, u, v \in \mathbb{C} \right\}$$

It is straightforward to check that this is a ring, but as $\left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right] \neq \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right]$, it is not commutative.

**Lemma 1.4.4.** If $a \in R$ is a unit, then $a$ is not a zero divisor.

*Proof:* Lat $ac = ca = 1$. Now suppose that $a$ is a zero divisor, so there exists a non-zero $b \in R$ with $ab = 0$. Then we have $cab = c(ab) = a \cdot 0 = 0$ but also $cab = (ca)b = 1 \cdot b = b \neq 0$. This is a contradiction, hence $a$ is not a zero divisor. ■

**Proposition 1.4.5.**

$$\text{Fields} \subsetneq \text{Integral domains} \qquad \text{and} \qquad \text{Finite integral domain} = \text{Field}$$

*Proof:* A field is a commutative ring where every non-zero element is a unit. As units are not zero divisors, a field has no zero divisors, is commutative, and has unity.

For the second statement, let $R$ be a finite integral domain, so $R = \{x_0, x_1, \ldots, x_n\}$ with $x_0 = 0$ and $x_1 = 1$. For some $k \in \{1, \ldots, n\}$, we have that the set $\{x_k x_1, \ldots, x_k x_n\} \subset R$ does not contain the zero element, as $R$ has no zero divisors. And since $x_k x_p = x_k x_q$ implies $x_p = x_q$, the list has all distinct elements, and is all of $R \setminus \{0\}$. Hence there is $\ell \in \{1, \ldots, n\}$ such that $x_k x_\ell = 1$, so $x_\ell$ is the inverse of $x_k$. Since $x_k$ was arbitrary, every element has an inverse. ■

**Definition 1.4.6.** A ring $R$ has characteristic $n$ if for all $a \in R$, $n \in \mathbb{N}$ is the smallest element such that $n \cdot a = 0$. This relation is expressed $\text{char}(R) = n$. If no such $n$ exists, then $\text{char}(R) = 0$.

**Example 1.4.7.** These are some examples of characteristics.

1. $\text{char}(\mathbb{Z}_n) = \dfrac{n}{\gcd\{1, 2, \ldots, n-1\}}$
2. $\text{char}(\mathbb{R}) = 0$

**Theorem 1.4.8.** If $R$ is an integral domain or a field, then $\text{char}(R) \in \mathbb{P} \cup \{0\}$ where $\mathbb{P}$ is the set of primes.

## 1.5 Homomorphisms

**Definition 1.5.1.** A function $\varphi : R_1 \to R_2$ on rings is termed a ring homomorphism iff for all $a, b \in R$,

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$

A ring homomorphism is completely determined by $\varphi(1)$.

**Example 1.5.2.** These are some examples of ring homomorphisms, for rings $R_1, R_2$.

1. $\varphi : R_1 \to R_2$ given by $\varphi(a) = a$
2. $\varphi : R_1 \to R_2$ given by $\varphi(a) = 0$

In the case where $R_1 = R_2 = \mathbb{Z}_{12}$, there are several unique ring homomorphisms. The choice of $a$ in $\varphi(1) = a$ is limited by the fact that in $\mathbb{Z}_{12}$, $a = \varphi(1) = \varphi(1)\varphi(1) = a^2$, and here only $a = 0, 1, 4, 9$ satisfies this property.

$\varphi(1) = 0$: Then $\varphi(n) = 0$ for all $n \in \mathbb{Z}_{12}$
$\varphi(1) = 1$: Then $\varphi(n) = n$ for all $n \in \mathbb{Z}_{12}$. This is the trivial homomorphism.
$\varphi(1) = 4$: Then $\varphi(\mathbb{Z}_{12}) = \{0, 4, 8\}$
$\varphi(1) = 9$: Then $\varphi(\mathbb{Z}_{12}) = \{0, 3, 6, 9\}$

**Definition 1.5.3.** Given a ring homomorphism $\varphi : R_1 \to R_2$, define the kernel of $\varphi$ to be the set

$$\ker(\varphi) = \{a \in R_1 \mid \varphi(a) = 0\}$$

**Theorem 1.5.4.** Let $\varphi : R_1 \to R_2$ be a ring homomorphism. Then for all $a, b \in R_1$ and $n \in \mathbb{N}$,

1. $\varphi(0) = 0$ and $\varphi(-a) = -\varphi(a)$
2. $\varphi(na) = n\varphi(a)$
3. $\varphi(a^n) = \varphi(a)^n$, for $n \in \mathbb{N}$ ($n \in \mathbb{Z}$ if $a$ is a unit)
4. $\varphi$ is 1-1 iff $\ker(\varphi) = \{0\}$
5. If $A \ll R_1$, then $\varphi(A) \ll \varphi(R_1)$
6. If $B \ll \varphi(R_1)$, then $\varphi^{-1}(B) \ll R_1$
7. $\varphi(1)$ is unity in $\varphi(R_1)$
8. $\ker(\varphi) \ll R_1$
9. If $R_1$ has unity / is commutative / is a division ring, so is $\varphi(R_1)$

*Proof:* Exercise. ■

**Definition 1.5.5.** If $\varphi : R_1 \to R_2$ is an injective homomorphism, then $\varphi$ is termed an isomorphism, and $R_1$ and $R_2$ are termed isomorphic. This relation is denoted by $R_1 \approx R_2$. Moreover, $\approx$ is an equivalence relation.

**Example 1.5.6.** The set $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ is isomorphic to $\mathbb{Q}[i]$ by $\varphi(a + bi) = \varphi(a - bi)$.

**Proposition 1.5.7.** Let $R_2 \approx R_2$. Then $R_1$ has the following properties iff $R_2$ does.

1. commutativity
2. having unity
3. being an integral domain
4. being a division ring
5. being a field
6. having a specific characteristic

**Example 1.5.8.** The above proposition makes it easier to inspect a structure by finding an isomorphic structure. For example, take

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\} \subset M(2, \mathbb{R})$$

We claim that $R \approx \mathbb{C}$ by $\varphi\left(\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right]\right) = a + bi$. The proof is left as an exercise.

# 2 Ideals and polynomial rings

## 2.1 Ideals

**Definition 2.1.1.** If $I \ll R$ for $R$ a ring, such that for all $a \in I$ and $b \in R$ we have that $ab, ba \in I$, then $I$ is termed an ideal of $R$.

**Example 2.1.2.** Consider some rings and their respective ideals.

1. The ring $\mathbb{Z}$ has ideals $n\mathbb{Z} = \{n \cdot m \mid m \in \mathbb{Z}\}$ for all $n \in \mathbb{N}$.
2. The ring $\mathbb{Z}_{12}$ has ideals

$$\begin{array}{lll} \{0\} & \{0,4,8\} & \{0,2,4,6,8,10\} \\ \{0,6\} & \{0,3,6,9\} & \{0,1,2,3,4,5,6,7,8,9,10,11\} \end{array}$$

3. The ring $\mathbb{Z}_n$ has ideals $\{I_a = \{m \cdot a \mid m \in \mathbb{N}, m \cdot a \leqslant n\} \mid a \text{ divides } n\}$
4. The ring $\mathbb{Q}$ has lots of subrings (such as $\mathbb{Z}$ and $2\mathbb{Z}$), but the only ideals are $\{0\}$ and $\mathbb{Q}$

**Definition 2.1.3.** Let $R$ be a commutative ring. Then the ideal $\langle a \rangle = \{ar \mid r \in R\}$ is termed the ideal generated by $a \in R$.

**Theorem 2.1.4.** Let $R$ be a commutative ring with unity whose only ideals are $R$ and $\{0\}$. Then $R$ is a field.

*Proof:* It must be shown that every non-zero element is a unit. Take $a \neq 0$ in $R$ and consider $\langle a \rangle$. Since the only ideals of $R$ are $\{0\}$ and $R$, it must be that $\langle a \rangle = R$. Since $1 \in R$, we have that $1 \in \langle a \rangle$, and so there exists $b \in R$ such that $ab = 1$, and so $a$ is a unit. ■

**Theorem 2.1.5.** Let $\varphi : R_1 \to R_2$ be a homomorphism. Then $\ker(\varphi)$ is an ideal of $R$.

*Proof:* Let $a \in \ker(\varphi)$. We need to show for all $b \in R$ that $ab, ba \in \ker(\varphi)$. Observe that $\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot \varphi(b) = 0$. Similarly for $\varphi(ba)$, it is clear that $ab, ba \in \ker(\varphi)$. ■

**Corollary 2.1.6.** If $F$ is a field, then all non-trivial homomorphisms of $F$ into itself are injective.

**Example 2.1.7.** Consider $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2$ given by $\varphi(a) = a \pmod 2$ (this is termed the natural homomrphism). Then $\ker(\varphi) = \{0, 2, 4\}$, which must be an ideal of $\mathbb{Z}_6$.

**Definition 2.1.8.** Let $R$ be a ring with an ideal $I$. Then the set $\mathbb{R}/I = \{a + I \mid a \in R\}$ where $a + I = \{a + b \mid b \in I\}$ is termed a quotient ring of $R$. We define addition and multiplication in this ring, for all $a, b \in R/I$, by:

$$\begin{aligned} (a+I) + (b+I) &= (a+b) + I \\ (a+I)(b+I) &= ab + I \\ a + I &= 0 + I \iff a \in I \end{aligned}$$

**Example 2.1.9.** Consider the ideal $\{0,2,4\}$ in $\mathbb{Z}_6$ and the ring $\{a+\{0,2,4\} \mid a \in \mathbb{Z}_6\} = \{\{0,2,4\},\{1,3,5\}\}$, for which

| $+$ | {0,2,4} | {1,3,5} |
|---|---|---|
| {0,2,4} | {0,4,2} | {1,5,3} |
| {1,3,5} | {1,5,3} | {2,0,4} |

| $\cdot$ | {0,2,4} | {1,3,5} |
|---|---|---|
| {0,2,4} | {0,2,4} | {1,3,5} |
| {1,3,5} | {1,3,5} | {0,2,4} |

**Theorem 2.1.10.** Let $R$ be a ring with an ideal $I$. Then $\varphi : R \to R/I$ is a ring homomorphism, with $\ker(\varphi) = I$.

*Proof:* Since the map is clearly surjective, it remains to prove that $\ker(\varphi) = I$. Recall that $\varphi(0) = 0 + I$ is the zero element in $R/I$. Now suppose that $\varphi(a) = a + I = 0 + I$, so there exists a $b \in I$ such that $a + b = 0$. Since $b \in I$, we also have that $-b \in I$, and hence $a \in I$. ■

**Definition 2.1.11.** Let $I$ be an ideal of a ring $R$. Then the ring $R/I$ is termed the quotient ring of $R$ with respect to $I$.

Many properties of $R$ (including commutativity and unity) carry over from $R$ to $R/I$.

**Theorem 2.1.12.** [First isomorphism theorem for rings]
Let $\varphi : R_1 \to R_2$ be a homomorphism. Then $R_1/\ker(\varphi) \approx \varphi(R_1)$.

*Proof:* We must find a bijective homomorphism $\chi : R_1/\ker(\varphi) \to \varphi(R_1)$. We claim that $\chi$ given by $\chi(a + \ker(\varphi)) = \varphi(a)$ will work. First note that

$$\chi((a+\ker(\varphi))(b+\ker(\varphi))) = \chi(ab+\ker(\varphi)) = \varphi(a)\varphi(b) = \chi(a+\ker(\varphi))\chi(b+\ker(\varphi))$$

Addition is checked similarly. The map $\chi$ is clearly surjective, as for any element $\varphi(a) \in \varphi(R_1)$, we have $\chi(a + \ker(\varphi)) = \varphi(a)$. Now suppose that $\chi(a + \ker(\varphi)) = \chi(b + \ker(\varphi))$, so then

$$\begin{aligned} \varphi(a) &= \varphi(b) \\ \varphi(a) - \varphi(b) &= 0 \\ \varphi(a) + \varphi(-b) &= 0 \\ \varphi(a-b) &= 0 \\ a - b &\in \ker(\varphi) \\ a &\in b + \ker(\varphi) \end{aligned}$$

Similarly we find that $b \in a + \ker(\varphi)$, so $a + \ker(\varphi) = b + \ker(\varphi)$. Hence $\chi$ is injective, and hence a bijection, and hence an isomorphism. ■

**Theorem 2.1.13.** Let $I, J$ be ideals of a ring $R$ with $I \subsetneq J \subsetneq R$. Let $\varphi : R \to R/I$ be given by $\varphi(a) = a + I$. Then $\varphi(J)$ is an ideal of $R/I$.

*Proof:* Let $a = \alpha + I \in \varphi(J)$ and $b = \beta + I \in R/I$. Then we have that $\alpha \in J$. Then $ab = \alpha\beta + I$, and $\alpha\beta \in J$, as $J$ is an ideal of $R$ and $\beta \in R$. Similarly, $ba = \beta\alpha + I$, and $\beta\alpha \in J$, again as $J$ is an ideal of $R$ and $\beta \in R$. Hence $ab, ba \in \varphi(J)$. ■

**Definition 2.1.14.** Let $I$ be a non-trivial ideal of $R$ (i.e. $I \neq R$) with no ideal $J$ of $R$ with $I \subsetneq J \subsetneq R$. Then $I$ is termed a maximal ideal of $R$.

**Definition 2.1.15.** Let $R$ be a commutative ring with an ideal $I$. If for all $a, b \in R$ with $ab \in I$ either $a \in I$ or $b \in I$, then $I$ is termed a prime ideal of $R$.

**Example 2.1.16.** Consider the following examples:
- $R = \mathbb{Z}$ - the ideal $p\mathbb{Z}$ is a maximal (and prime) ideal for all $p$ prime
- $R = \mathbb{Z} \times \mathbb{Z}$ - the ideal $\{(a, 0) \mid a \in \mathbb{Z}\}$ is a prime ideal, but $\{(3a, 2b) \mid a, b \in \mathbb{Z}\}$ is maximal
- $R = \mathbb{Z} \times \mathbb{Z}$ - the ideal $2\mathbb{Z} \times 2\mathbb{Z}$ is neither prime nor maximal, but $(\mathbb{Z} \times \mathbb{Z})/(2\mathbb{Z} \times 2\mathbb{Z}) \approx \mathbb{Z}_2 \times \mathbb{Z}_2$

Note that $\{\text{maximal ideal of } R\} \subsetneq \{\text{prime ideal of } R\} \subsetneq \{\text{ideal of } R\}$.

**Theorem 2.1.17.** Let $R$ be a commutative ring with unity. Then
1. $I$ is a prime ideal iff $R/I$ is an integral domain
2. $I$ is a maximal ideal iff $R/I$ is a field

*Proof:* **1.** Let $I$ be a prime ideal. Suppose that $R/I$ is not an integral domain. As $R/I$ is a commutative ring with unity, we must have a zero divisor $(a + I)(b + I) = I$, but $(a + I)(b + I) = ab + I = I$, so then $ab \in I$. Since $I$ is a prime ideal, $a \in I$ or $b \in I$, so $a + I = I$ or $b + I = I$. This contradicts both being zero divisors, as they are then 0 in $R/I$, and hence $R/I$ is an integral domain.

Reverse direction is similar.

**2.** Suppose that $R/I$ is a field but not a maximal ideal, so there exists an ideal $J$ of $R$ with $I \subsetneq J \subsetneq R$. Let $\varphi : R \to R/I$ be given by $\varphi(a) = a + I$. We know that $\varphi(J)$ is not a trivial ideal of $R$, but the only ideals of fields are $\{0\}$ and the field. This is a contradiction, hence $I$ is maximal.

Reverse direction is similar. ■

## 2.2 The field of quotients

**Definition 2.2.1.** Let $R$ be an integral domain. The field $FQ(R) = \{\frac{a}{b} \mid a, b \in R, b \neq 0\}/\sim$ is termed the field of quotients of $R$, for $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$ .

**Example 2.2.2.** Here are some examples of rings and their fields of quotients.
1. $R = \mathbb{Z}$, $FQ(R) = \mathbb{Q}$
2. $R = \mathbb{Z}[i]$, $FQ(R) = \mathbb{Q}[i]$
3. $R = Z_p$, $FQ(R) = \mathbb{Z}_p$

The last example shows that if $R$ is a field, then $R \approx FQ(R)$.

**Theorem 2.2.3.** Any field $F$ that contains a nontrivial integral domain $D$ as a subring (in particular $\{n \cdot 1 \mid n \in \mathbb{Z}\}$) contains an isomorphic copy of $FQ(D)$, or

$$D \subset FQ(D) \subset F$$

## 2.3 Polynomial rings

**Definition 2.3.1.** Let $R$ be a ring. Define the ring of polynomials of $R$ to be

$$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{R}, n \in \mathbb{N} \right\}$$

Addition and multiplication are defined in $R[x]$ in the obvious way.

$$\left( \sum_{i=0}^{n} a_i x^i \right) \left( \sum_{j=0}^{m} b_j x^j \right) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j} = \sum_{k=0}^{n+m} \left( \sum_{i+j=k} a_i b_j \right) x^k$$

The indeterminate $x$ is assumed to commute with everything. Note that $R[x]$ is not necessarily commutative.

**Remark 2.3.2.** The ring $R[x]$ inherits some properties from $R$:

· commutativity
· having unity
· having/not having zero divisors

Others it does not necessarily inherit:

· being a division ring
· being a field

**Definition 2.3.3.** The set of formal power series over a ring $R$ is defined as

$$R[[x]] = \left\{ \sum_{i=1}^{\infty} a_i x^i \mid a_i \in \mathbb{R} \right\}$$

The radius of convergence is not pertinent to the study of such structures. Note also that $R[x] \ll R[[x]]$.

**Definition 2.3.4.** Let $F$ be a field with $f(x), g(x) \in F[x]$. Then we write

$$f(x) \,\big|\, g(x) \quad \iff \quad \text{there exists } h(x) \in F[x] \text{ with } f(x)h(x) = g(x)$$

**Definition 2.3.5.** For $f(x), g(x) \in F[x]$, an element $d(x) \in F[x]$ is termed the gcd of $f(x)$ and $g(x)$ iff

**1.** $d(x) \mid f(x)$ and $d(x) \mid g(x)$
**2.** if $e(x) \in F[x]$ is such that $e(x) \mid f(x)$ and $e(x) \mid g(x)$, then $d(x) \mid e(x)$

Note that gcds are not unique.

**Theorem 2.3.6.** For $f(x), g(x) \in F[x]$ with $g$ nonzero, there exist unique $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$, with $\deg(r) < \deg(g)$, where $\deg(0) = -\infty$.

*Proof:* It is necessary to show that there exists a unique solution to $f(x) = q(x)g(x) + r(x)$. Now suppose that $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$. Then $g(x)(q_2(x) - q_1(x)) = r_2(x) - r_1(x)$. But this is a contradiction, as the degrees of both sides of the equality do not match. This proves uniqueness.

Now, let $f(x) = \sum_{i=1}^{n} a_i x^i$ and $g(x) = \sum_{i=1}^{k} b_i x^i$ and proceed by induction on $n$. If $f(x) = 0$, use $q(x) = r(x) = 0$. If $\deg(f) < \deg(g)$, let $q(x) = 0$ and $r(x) = f(x)$. Otherwise, define $f'(x) = f(x) - a_n b_k^{-1} x^{n-k} g(x)$, so $\deg(f') \leqslant n - 1$. Applying induction, we may write

$$\begin{aligned} f'(x) &= g(x)q'(x) + r'(x) \\ f(x) - a_n b_k^{-1} x^{n-k} g(x) &= g(x)q'(x) + r'(x) \\ f(x) &= g(x) \underbrace{(a_n b_k^{-1} x^{n-k} + q'(x))}_{q(x)} + \underbrace{r'(x)}_{r(x)} \end{aligned}$$

This proves existence. ■

**Theorem 2.3.7.** For $f(x), g(x) \in F[x]$, there exist $a(x), b(x) \in F[x]$ such that $f(x)a(x) + g(x)b(x) = \gcd(f(x), g(x))$.

*Proof:* Consider the ideal $I = \langle f(x), g(x) \rangle$ of $F[x]$. Let $d(x) \in I$ nonzero be of minimal degree. We claim that $d(x) = \gcd(f(x), g(x))$.

To show that $d(x)$ is a common divisor, first write $f(x) = d(x)q(x) + r(x)$ with $\deg(r) < \deg(f)$. Note $r(x) = f(x) - d(x)q(x)$, so $r(x) \in I$. Hence $r(x) = 0$, as $d$ is of minimal degree. Therefore $d(x) \mid f(x)$ and similarly $d(x) \mid g(x)$, so write $d(x) = a(x)f(x) + b(x)g(x)$.

To see that $d(x)$ is the *greatest* common divisor, first suppose that $c(x) \mid f(x)$ and $c(x) \mid g(x)$, so

$$\begin{aligned} d(x) &= a(x)f(x) + b(x)g(x) \\ &= a(x)(c(x)a'(x)) + b(x)(c(x)b'(x)) \\ &= c(x)(a(x)a'(x) + b(x)b'(x)) \\ &\implies d(x) \mid c(x) \end{aligned}$$

This proves the theorem. ■

## 2.4 Polynomial irreducibility

**Definition 2.4.1.** Let $F$ be a field with $f(x) \in F[x]$. Then $f(a) = 0$ iff $(x-a) \,\big|\, f(x)$. Such an $a$ is termed a root of $f(x)$.

**Theorem 2.4.2.** Let $F$ be a field with $f(x) \in F[x]$. If $f(x)$ has degree $n$, then it has at most $n$ roots.

*Proof:* By induction. If $a$ is a root, then $f(x) = (x-a)q(x)$, and $q(x)$ has at most $n-1$ roots. ■

**Corollary 2.4.3.** Let $D$ be an integral domain. If $f(x) \in D[x]$ has degree $n$, then it has at most $n$ roots.

*Proof:* Let $F = FQ(D)$, the field of quotients of $D$, so $f(x) \in D[x] \subset F[x]$. As $f(x)$ has at most $n$ roots in $F[x]$, it has at most $n$ roots in $D[x]$. ■

**Definition 2.4.4.** We say that $f(x) \in D[x]$ is reducible if $f(x) = g(x)h(x)$ for $g, h$ non-constant. If no such $g, h$ exist, then $f$ is termed irreducible.

**Theorem 2.4.5.** Let $F$ be a field. Then $f(x) \in F[x]$ can be written uniquely as a constant multiplied by a product of monic irreducible polynomials, $f(x) = u \cdot q_1(x)q_2(x)\cdots q_k(x)$.

*Proof:* We proceed by induction. To show such a reperesentation exists, we consider a number of cases.
Case 1: $f(x) = 0$. Then use $u = 0$ and $k = 0$.
Case 2: $f(x) = c$ for $c$ a constant. Then use $u = c$ and $k = 0$.
Case 3: $\deg(f) = 1$. If $f(x) = ax + b$, use $u = a$ and $k = 1$ with $q_a(x) = 1 + \frac{b}{a}x$.
Case 4: $\deg(f) > 1$ and $f$ is irrdeucible. If $f(x) = \sum_{i=1}^{n} a_i x^i$, use $u = a_n$ and $k = 1$ with $q_1(x) = \frac{f(x)}{a_n}$.
Case 5: $\deg(f) > 1$ and $f$ is reducible. If $f(x) = g(x)h(x)$, use induction, as $\deg(g), \deg(h) < \deg(f)$.

To show uniqueness, suppose that $f(x) = u \cdot q_1(x)\cdots q_k(x) = v \cdot p_1(x)\cdots p_\ell(x)$. Since all the factors are monic, $u = v$. As $q_1 \mid f$, we have that $q_1 \mid p_1 \cdots p_\ell$. Since $q_1$ is irreducible and all $p_i$ are irreducible, $q_1$ divides exactly one $p_i$. Repeat this for all $q_i$ to show that $k = \ell$, and for each $i \in \{1, \ldots, k\}$, there is a unique $j_i \in \{1, \ldots, k\}$ such that $q_i = p_{j_i}$ iff $i = j$. ■

**Theorem 2.4.6.** Let $F$ be a field and $f(x) \in F[x]$ of degree 2 or 3. Then $f$ is irreducible iff it has no roots, i.e. $f(a) \neq 0$ for all $a \in F$.

**Theorem 2.4.7.** [Rational root theorem]
Let $F$ be a field with $f(x) = \sum_{i=1}^{n} a_i x^i \in F[x]$. If $f(x)$ has a root $\frac{r}{s} \in \mathbb{Q}$ with $\gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

*Proof:* Observe that

$$0 = s^n f\left(\frac{r}{s}\right) = a_0 s^n + a_1 s^{n-1} r + a_2 s^{n-2} r^2 + \cdots + a_n r^n \equiv a_0 s^n \pmod{r} \implies r \mid a_0$$

In a symmetric way $s \mid a_n$. ■

**Theorem 2.4.8.** [Eisenstein]
Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ such that there exists $p$ prime with:
- $p \nmid a_n$
- $p \mid a_i$ for all $i = 0, 1, \ldots, n-1$
- $p^2 \nmid a_0$

Then $f(x)$ is irreducible.

*Proof:* Suppose the conditions are satisfied, but $f$ is reducible. Then $f(x) = g(x)h(x)$ for $g(x) = \sum_{i=0}^{k} b_i x^i$ and $h(x) = \sum_{i=0}^{\ell} c_i x^i$ for $k, \ell \neq 0$, with $a_0 = b_0 c_0$. The assumptions of the theorem imply that $p \mid b_0$ xor $p \mid c_0$, and WLOG $p \mid b_0$ and $p \nmid c_0$. Since $p \nmid a_n$ and $a_n = b_k c_\ell$, we have that $p \nmid b_k$ and $p \nmid c_\ell$.

Consider $\varphi(f)$ for $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ a homomorphism. Then $\varphi(f(x)) = a_n x^n$ and $\varphi(g(x)) = \sum_{i=1}^{k} b_i x^i$ and $\varphi(h(x)) = \sum_{i=0}^{\ell} c_i x^i$ with $c_0 \neq 0$. Let $b_t$ be the first term in $\{b_0, \ldots, b_k\}$ with $b_t \neq 0 \pmod{p}$. So then $\varphi(g(x)) = \sum_{i=t}^{k} b_i x^i$, and $\varphi(g(x)h(x)) = b_t c_0 x^t + \cdots + b_k c_\ell x^{k+\ell}$. But $t < n$, as $t \leqslant k \leqslant n-1$, so $\varphi(g(x)h(x)) \neq \varphi(g(x))\varphi(h(x))$, contradicting that $\varphi$ is a homomorphism. Therefore the original assumption was false, and so $f(x)$ is irreducible. ■

**Theorem 2.4.9.** Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ be the natural homomorphism for $p$ prime and $f(x) \in \mathbb{Z}[x]$. If $\deg(f) = \deg(\varphi(f))$ and $\varphi(f)$ is irreducible in $\mathbb{Z}_p[x]$, then $f$ is irreducible in $\mathbb{Z}[x]$.

*Proof:* Suppose that the conditions of the theorem hold, but $f(x) = g(x)h(x)$ for $g, h$ nonconstant in $\mathbb{Z}[x]$. Then $\varphi(f(x)) = \varphi(g(x))\varphi(h(x))$, and as $\deg(f(x)) = \deg(\varphi(f(x)))$, the lead coefficient of $f(x)$ is not divisible by $p$. Therefore the lead coefficients of both $g(x)$ and $h(x)$ are not divisible by $p$. Hence $\varphi(g(x))$ and $\varphi(h(x))$ are non-trivial factors of $\varphi(f(x))$, leading to a contradiction. Hence $f(x)$ is irreducible in $\mathbb{Z}[x]$. ■

# 3 PIDs, EUDs, and UFDs

## 3.1 Principal ideal domains

**Definition 3.1.1.** Let $R$ be a commutative ring. Then define the ideal generated by $A$ for $A = \{a_1, \ldots, a_n\} \subset R$ to be the set

$$\langle a_1, \ldots, a_n \rangle = \left\{ \sum_{i=1}^{n} a_i b_i \mid b_i \in R \ \forall \ i \right\}$$

**Example 3.1.2.** For $R = \mathbb{Z}$, we have that $\langle a_1, \ldots, a_n \rangle = \langle \gcd(a_1, \ldots, a_n) \rangle$.

**Definition 3.1.3.** Let $D$ be an integral domain. If every ideal in $D$ can be expressed as $I = \langle a \rangle$ for some $a \in D$, then $D$ is termed a principal ideal domain.

**Example 3.1.4.**
- $\mathbb{Z}$ is a PID, as $n\mathbb{Z} = \langle n \rangle$
- $\mathbb{Z}[x]$ is not a PID, as $\langle x+1, 2 \rangle$ can not be written as $\langle f(x) \rangle$

**Theorem 3.1.5.** Let $F$ be a field. Then $F[x]$ is a PID.

*Proof:* Since $F[x]$ is a field, any ideal $I$ of $F[x]$ is either $\{0\}$ or has a non-zero element. In the first case, $I = \langle 0 \rangle$. In the second case, we claim that $I = \langle g(x) \rangle$ for $g(x)$ a non-zero element of minimal degree in $I$.

For any $f(x) \in I$, the division algorithm gives us that there exist $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$, with $\deg(r) < \deg(g)$. Since $f(x)$ and $q(x)g(x) \in I$, we have that $r(x) \in I$. Since $g(x)$ had minimal degree in $I$, $r(x) = 0$, so $g(x) \mid f(x)$ and $f(x) = q(x)g(x) \in \langle g(x) \rangle$. Hence all elements in $I$ are in $\langle g(x) \rangle$, and $g(x) \in I$, so $I = \langle g(x) \rangle$. Therefore $\mathbb{F}[x]$ is a PID. ■

**Theorem 3.1.6.** Let $F$ be a field with $f(x) \in F[x]$. Then $\langle f(x) \rangle$ is a prime ideal iff $f(x)$ is irreducible.

*Proof:* Suppose that $\langle f(x)\rangle$ is a prime ideal and $f(x) = g(x)h(x)$ for $g, h$ nonconstant. Since $\deg(g), \deg(h) < \deg(f)$, by the proof above we have that $g(x), h(x) \notin \langle f(x)\rangle$. But $g(x)h(x) \in \langle f(x)\rangle$, so either $g(x) \in \langle f(x)\rangle$ or $h(x) \in \langle f(x)\rangle$, contradicting the above. Therefore $f(x)$ is irreducible.

Suppose that $f(x)$ is irreducible, and $g(x)h(x) \in \langle f(x)\rangle$. It remains to show that either $g(x) \in \langle f(x)\rangle$ or $h(x) \in \langle f(x)\rangle$. Since $g(x)h(x) \in \langle f(x)\rangle$, we have that $g(x)h(x) = p(x)f(x)$ for some $p(x) \in \mathbb{F}[x]$, and so

$$f(x) \mid g(x)h(x) = u \cdot g_1(x) \cdots g_n(x) \cdot v \cdot h_1(x) \cdots h_m(x) \implies f(x) \mid k(x) \text{ for } k \in \{g_1, \ldots, g_n, h_1, \ldots, h_m\}$$

If $f(x) \mid g_i(x)$, then $g(x) \in \langle f(x)\rangle$, and if $f(x) \mid h_i(x)$, then $h(x) \in \langle f(x)\rangle$, so $\langle f(x)\rangle$ is a prime ideal. ■

**Corollary 3.1.7.** Let $\mathbb{F}$ be a field with $\mathbb{F}[x] \ni g(x)$. Then equivalently, in $\mathbb{F}[x]$:
- $\langle g(x)\rangle$ is a maximal ideal
- $\langle g(x)\rangle$ is a prime ideal
- $g(x)$ is irreducible

*Proof:* Over an integral domain, maximal ideals are prime and prime ideals are maximal. ■

**Example 3.1.8.** In $\mathbb{Q}[x]$, $x^2+1$ is irreducible, so $\langle x^2+1\rangle$ is a maximal and prime ideal, so $\mathbb{Q}[x]/\langle x^2+1\rangle \approx \mathbb{C}[x]$ is a field.

**Definition 3.1.9.** Let $R$ be a ring with an ideal $I$. Then we write $a \equiv b \pmod{I}$ iff $a - b \in I$.

**Theorem 3.1.10.** For ideals $I_1, I_2$ of a ring $R$, if $I_1 \subset I_2 \subset R$ and $a \equiv b \pmod{I}_1$, then $a \equiv b \pmod{I}_2$.

*Proof:* Simply observe that

$$\begin{aligned} a \equiv b \pmod{I_1} &\implies a - b \in I_1 \\ &\implies a - b \in I_2 \\ &\implies a \equiv b \pmod{I_2} \end{aligned}$$

■

**Example 3.1.11.** For $\mathbb{Z}_2[x]/\langle x^2+2\rangle$, we have $\langle x^2+2\rangle \subset \langle x\rangle$ and $\langle x^2+2\rangle \subset \langle x+1\rangle$. Then we have maps
- $\varphi_1 : \mathbb{Z}_2[x]/\langle x^2+x\rangle \to \mathbb{Z}_2[x]/\langle x\rangle$ by $ax + b + \langle x^2+2\rangle \mapsto ax + b + \langle x\rangle = b + \langle x\rangle$
- $\varphi_2 : \mathbb{Z}_2[x]/\langle x^2+x\rangle \to \mathbb{Z}_2[x]/\langle x+1\rangle$ by $ax + b + \langle x^2+2\rangle \mapsto a + b + \langle x+1\rangle$

**Theorem 3.1.12.** For ideals $I_1, I_2$ of a ring $R$, if $I_1 \subset I_2 \subset R$, then the map $\varphi : R/I_1 \to R/I_2$ given by $\varphi(a + I_1) = a + I_2$ is a ring homomrphism.

**Theorem 3.1.13.** Let $F$ be a field and $\gcd(f(x), g(x)) = 1$ for $f(x), g(x) \in F[x]$. Then

$$F[x]/\langle f(x), g(x)\rangle \approx F[x]/\langle f(x)\rangle \times F[x]/\langle g(x)\rangle$$

*Proof:* Relabel the above $A \approx B \times C$. The existence of a homomorphism $\varphi$ from $A$ to $B \times C$ is given by the previous theorem, so it remains to show that the homomorphism is bijective.

Suppose that $\varphi(a) = (b, c) = \varphi(d)$, so we must show that $a = d$. Consider

$$\begin{aligned} a(x) \equiv d(x) \pmod{\langle f(x)\rangle} &\implies a(x) - d(x) \in \langle f(x)\rangle \\ &\implies f(x) \mid (a(x) - d(x)) \\ &\implies a(x) - d(x) = f(x)p(x) \end{aligned}$$

Similarly $a(x) \equiv d(x) \pmod{\langle g(x)\rangle}$ implies that $a(x) - d(x) = g(x)q(x)$ for some $q(x)$. Hence $f(x)p(x) = g(x)q(x)$ for some polynomials $p, q$, and as $\gcd(f(x), g(x)) = 1$, $f(x) \mid q(x)$, hence $q(x) = f(x)k(x)$. So $a(x) - d(x) = g(x)q(x) = g(x)f(x)k(x) \in \langle f(x)g(x)\rangle$. Hence

$$a(x) + \langle f(x)g(x)\rangle = d(x) + \langle f(x)g(x)\rangle$$

as required. It remains to show that $\varphi$ is surjective. So we must show that for $(a(x)+\langle f(x)\rangle, b(x)+\langle g(x)\rangle)$, there exists $c(x)+\langle f(x)g(x)\rangle$ such that $\varphi(c(x)+\langle f(x)g(x)\rangle) = (a(x)+\langle f(x)\rangle, b(x)+\langle g(x)\rangle)$.

So first recall that $\gcd(f(x), g(x)) = 1$, so there exist $h(x), k(x) \in F[x]$ such that $f(x)h(x)+g(x)k(x) = 1$. Define $c(x)$ to be the polynomial

$$c(x) = a(x)g(x)k(x) + b(x)f(x)h(x) + \langle f(x)g(x)\rangle \in F[x]/\langle f(x)g(x)\rangle$$

for which

$$c(x) \equiv a(x)g(x)k(x) \pmod{\langle f(x)\rangle} \equiv a(x)(1-f(x)h(x)) \pmod{\langle f(x)\rangle} \equiv a(x) \pmod{\langle f(x)\rangle}$$

Similarly $c(x) \equiv b(x) \pmod{\langle g(x)\rangle}$, which gives surjectivity. ■

**Example 3.1.14.** Consider the ring $\mathbb{Q}[x]/\langle x^4 - 3x^2 + 2\rangle$ for which

$$\begin{aligned}\mathbb{Q}[x]/\langle x^4-3x^2+2\rangle &= \mathbb{Q}[x]/\langle (x-1)(x+1)(x^2-2)\rangle \\ &\approx \mathbb{Q}[x]/\langle x-1\rangle \times \mathbb{Q}[x]/\langle (x+1)(x^2-2)\rangle \\ &\approx \mathbb{Q}[x]/\langle x-1\rangle \times \mathbb{Q}[x]/\langle x+1\rangle \times \mathbb{Q}[x]/\langle x^2-2\rangle \\ &\approx \mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\left[\sqrt{2}\right]\end{aligned}$$

## 3.2 Euclidean domains

**Definition 3.2.1.** Let $D$ be an integral domain. Suppose that there exists a function $v : D\setminus\{0\} \to \mathbb{N}\cup\{0\}$ such that for all $x, y \in D$,

· $v(x) \leqslant v(xy)$

· there exist $q, r \in D$ such that $x = qy + r$ and $v(r) < v(y)$ or $r = 0$

Then $D$ is termed a Euclidean domain, and $v$ is termed a Euclidean function.

**Example 3.2.2.** Consider the following examples of Euclidean domains.

· $\mathbb{Z}$ is a EUD using $v(a) = |a|$

· $F[x]$ is a EUD using $v(f(x)) = \deg(f(x)) + 1$

· $\mathbb{Z}[i]$ is a EUD using $v(a+bi) = a^2+b^2 = |a+bi|$

**Theorem 3.2.3.** $\{\text{EUD}\} \subset \{\text{PID}\}$

*Proof:* Let $D$ be a EUD and $I$ an ideal in $D$. We will show that $I = \langle x\rangle$ for some $x \in D$. If $I = \{0\}$, take $x = 0$. Otherwise, pick a nonzero $x \in I$ such that $v(x)$ is minimal. For $y \in I$, there exist $q, r \in D$ such that $y = qx + r$ and $v(r) < v(x)$. Since $y, qx \in I$, we have that $r \in I$, but then $v(r) = 0$, as $x$ was minimal in $I$. So $y = qx$ and $y \in \langle x\rangle$. Therefore $I = \langle x\rangle$. ■

**Theorem 3.2.4.** Let $D \ni a, b$ be a EUD with $d = \gcd(a, b)$. Then there exist $u, v \in D$ with $au + bv = d$.

*Proof:* Consider $I = \langle a, b\rangle$. As $d \mid a$ and $d \mid b$, we have that $d = au$ and $d = bv$ for some $u, v \in D$. Then $d = au + bv \in I$. ■

**Definition 3.2.5.** Let $R$ be a commutative ring with $u \in R$ a unit. Then if $a = bu$ for $a, b \in R$, the elements $a, b$ are termed associates.

**Theorem 3.2.6.** Let $D \ni a, b$ be an integral domain. For $g, g'$ gcds of $a, b$, we have that

· $\langle g\rangle = \langle g'\rangle$

· $g, g'$ are associates

*Proof:* **2.** As both $g, g'$ are gcds of $a, b$, they are both common divisors of $a, b$. In particular, $g \mid g'$ and $g' \mid g$, so $g = ug'$ and $g' = vg$. Hence $g = uvg$, so $uv = 1$, meaning $u$ and $v$ are units, in tun implying that $g$ and $g'$ are associates.

**1.** For $g''$ a gcd of $a, b$, we know that $\langle a, b\rangle = \langle g''\rangle$. Hence $g'' = wg$ for $w$ a unit, and $g'' = ac + bd$ for some $c, d \in D$. Hence $w^{-1}ca + w^{-1}db \in \langle a, b\rangle$, so $\langle g\rangle = \langle a, b\rangle$, and similarly $\langle g'\rangle = \langle a, b\rangle$. ■

**Theorem 3.2.7.** Let $D$ be a EUD with Euclidean function $v$. Then

**1.** $v(1) \leqslant v(a)$ for all nonzero $a \in D$

**2.** $v(1) = v(a)$ iff $a \in D$ is a unit

*Proof:* Recall that $v(x) \leqslant v(xy)$ for $x, y \neq 0$, so let $x = 1$ and $y = a$. For the second one, note that $v(1) \leqslant v(a) \leqslant v(aa^{-1}) = v(1)$. ■

## 3.3 Unique factorization domains

**Definition 3.3.1.** An integral domain $D$ is termed a unique factorization domain if every nonzero $a \in D$ may be expressed uniquely (up to permutation) as a product of irreducibles and a unit.

**Definition 3.3.2.** Recall the following definitions:

**1.** $p \in D$ is irreducible iff:
- $p \neq 0$, $p$ is not a unit, and
- $p = ab \implies a$ or $b$ is a unit

**2.** $p \in D$ is prime iff:
- $p \neq 0$, $p$ is not a unit, and
- $p = ab \implies p \mid a$ or $p \mid b$

**Example 3.3.3.**
- Let $F$ be a field. Then $F$ has no irreducibles nor primes.
- In $\mathbb{Z}$ and $F[x]$, all the primes are irreducible, and all the irreducibles are prime.
- Let $R = \{a_0 + a_2x^2 + a_3x^3 + \cdots \mid a_i \in F\}$ with $x^3$ irreducible. But $x^3 \mid x^4x^2$ with $x^3 \nmid x^4$ and $x^3 \nmid x^2$.

**Theorem 3.3.4.** Let $D \ni p$ be a UFD. If $p$ is prime, then $p$ is irreducible.

*Proof:* Suppose that $p$ is prime and reducible, i.e. that $p = ab$ for $a, b$ not units. As $p$ is prime, WLOG $p \mid a$, hence $a = pb'$ and $p = ab = pb'b$, so $b$ is a unit, a contradiction. Hence $p$ is irreducible. ■

**Example 3.3.5.**
- $\mathbb{Z}, \mathbb{Z}[x]$ are UFDs (but $\mathbb{Z}[x]$ is not a PID)
- $\mathbb{Z}[x, y, z] = ((\mathbb{Z}[x])[y])[z]$ is a UFD
- $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, as $21 = 7 \cdot 3 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$

**Theorem 3.3.6.** Let $D$ be a PID. Then $p \in D$ is irreducible iff $\langle p\rangle$ is a maximal ideal.

*Proof:* Suppose that $p$ is irreducible. Suppose there exists an ideal $I$ with $\langle p\rangle \subset I \subset D$, with $I \neq D$. Since $D$ is a PID, $I = \langle a\rangle$ for some $a \in D$, where $a$ is not a unit. Then $\langle p\rangle \subset \langle a\rangle \subset D$, so there exists $b \in D$ with $p = ab$. Since $p$ is irreducible, $b$ is a unit. So $a = pb^{-1}$, and hence $a \in \langle p\rangle$, so $\langle a\rangle = \langle p\rangle$, and $\langle p\rangle$ is maximal.

Suppose that $\langle p\rangle$ is a maximal ideal in $D$, and $p = ab$ for $a$ not a unit. Then $a \mid p$ and $\langle p\rangle \subset \langle a\rangle \subset D$, and as $a$ is not a unit, $\langle a\rangle \neq D$. Since $\langle p\rangle$ was maximal, $\langle a\rangle = \langle p\rangle$, and $a \in \langle p\rangle$, meaning there is $b' \in D$ with $a = pb' = abb'$, so $b$ is a unit. Hence $p$ is irreducible. ■

**Corollary 3.3.7.** Let $D$ be a PID. Then $p$ is prime iff $p$ is irreducible.

*Proof:* We know that $p$ is irreducible iff $\langle p \rangle$ is maximal iff $\langle p \rangle$ is prime iff $p$ is prime. ■

**Lemma 3.3.8.** Let $D$ be a PID with $I_1 \subset I_2 \subset I_3 \subset \cdots \subset D$ be a sequence of nested ideals. Then there exists $n \in \mathbb{N}$ such that for all $m \geqslant n$, $I_m = I_n$.

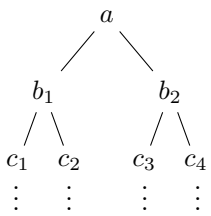
*Proof:* Let $I = \bigcup_j I_j = \{a \in D \mid a \in I_j \text{ for some } j\}$. Hence $I = \langle x \rangle$ for some $x \in D$, as $D$ is a PID. Thus $x \in I$ implies $x \in I_{n_0}$. Hence $\langle x \rangle \subset I_{n_0} \subset I_n \subset I = \langle x \rangle$ for all $n \geqslant n_0$. Hence $I_i = \langle x \rangle$ for all $i$. ■

**Theorem 3.3.9.** $\{\text{PID}\} \subset \{\text{UFD}\}$

*Proof:* We need to show that, for $D$ a PID,

1. For all $a \in D$, $a$ can be factored into a finite number of irreducibles
2. The factorization into irreducibles is unique up to rearangement and multiplication by units

Assume that $a$ is not irreducible, so $a = b_1 \cdot b_2$ for $b_1, b_2$ not units. If $b_1$ or $b_2$ are not irreducible, express them as $b_1 = c_1 \cdot c_2$ and $b_2 = c_3 \cdot c_4$, for all $c_i$ not units. Continue in this manner:




Claim 1: This factorization tree eventually stops.
To see this, first note that $\langle a \rangle \subset \langle b_2 \rangle \subset \langle c_4 \rangle \subset \cdots$. By the lemma, all branches are finite. Hence we have a representation $a = p_1 p_2 \cdots p_k$.

Claim 2: The representation $a = p_1 p_2 \cdots p_k$ is unique.
Suppose that $a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r$. As $D$ is a PID, all irreducibles are prime, meaning that

$$p_1 \mid a \implies p_1 \mid q_1 q_2 \cdots q_r \implies \exists\, j \in \{1, 2, \ldots, r\} \text{ such that } p_1 \mid q_j$$

So $q_j = p_1 \cdot u$, but as $q_j$ is irreducible, $u$ is a unit. Repeat this argument for $p_2 \cdots p_k = q_1 \cdots q_{j-1} q_{j+1} \cdots q_r$ to get that $p_2 \cdot v = q_\ell$ for some unit $v$. Repeat this $k$ times to get that $k = r$ and and the primes $p_i$ match up with the primes $q_i$. Hence the factorization is unique, and $D$ is a UFD. ■

**Definition 3.3.10.** For $D$ a UFD, an element $p(x) = a_n x^n + \cdots + a_0 \in D[x]$ is termed primitive iff $\gcd(a_n, \ldots, a_0) = 1$.

**Proposition 3.3.11.** For $D$ a UFD, if $p(x), q(x) \in D[x]$ are primitive in $D[x]$, then so is $p(x)q(x)$.

**Theorem 3.3.12.** Let $D$ be a UFD and $Q$ its field of quotients. Let $f(x) \in D[x] \subset Q[x]$ factor over $Q[x]$. Then $f(x)$ factors over $D[x]$.

*Proof:* WLOG assume that $f(x)$ is primitive with $f(x) = \left(\frac{a_n}{b_n} x^n + \cdots + \frac{a_0}{b_0}\right)\left(\frac{c_k}{d_k} x^k + \cdots + \frac{c_0}{d_0}\right)$, and let

$$\begin{array}{llll} a^* = & \gcd(a_n, \ldots, a_0) & c^* = & \gcd(c_k, \ldots, c_0) \\ b^* = & \operatorname{lcm}(b_n, \ldots, b_0) & d^* = & \operatorname{lcm}(d_k, \ldots, d_0) \\ a_i' = & (a_i \cdot b^*)/(b_i \cdot a^*) & c_i' = & (c_i \cdot d^*)/(d_i \cdot c^*) \end{array}$$

Then we have that $a_i/a^*, b^*/b_i \in D$ and $a_n' x^n + \cdots + a_0'$ is primitive, and so

$$f(x) = \frac{a^* c^*}{b^* d^*} \left(a_n' x^n + \cdots + a_0'\right)\left(c_k' x^k + \cdots + c_0'\right)$$

Then $\frac{b^*d^*}{a^*c^*}f(x)$ is primitive, and thus $\frac{b^*d^*}{a^*c^*} = u$ is a unit, and

$$f(x) = u^{-1}\left(a'_n x^n + \cdots + a'_0\right)\left(c'_k x^k + \cdots + c'_0\right)$$

Where $a'_i, c'_j \in D$ for all $i, j$, meaning that $f(x)$ factors over $D[x]$. ■

**Theorem 3.3.13.** If $D$ is a UFD, then $D[x]$ is a UFD.

*Proof:* Let $Q$ be the field of quotients of $D$. Then $Q$ is a field, hence $Q[x]$ is a UFD. Hence if $f(x) \in D[x] \subset Q[x]$, then it has a unique factorization in $Q[x]$, and so a unique factorization in $D[x]$. ■

# 4 Extension fields

## 4.1 The Gaussian integers

Recall that $\mathbb{Z}[i]$ is a UFD, so an element is irreducible if and only if it is prime.

· the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$
· if $n$ is not prime in $\mathbb{Z}$, then $n$ is not prime in $\mathbb{Z}[i]$ (the converse does not hold)
· for $v_{\mathbb{Z}}[i] \to \mathbb{N} \cup \{0\}$ given by $v(a+bi) = a^2 + b^2$, we have that $v(z) = 1$ iff $z$ is a unit

**Proposition 4.1.1.** If $v(z) \in \mathbb{P}$, then $z$ is irreducible.

**Proposition 4.1.2.** If $p \in \mathbb{P}$ and $p \equiv 3 \pmod 4$, then $p$ is prime in $\mathbb{Z}[i]$.

**Theorem 4.1.3.** If $p \equiv 1 \pmod 4$ for $p \in \mathbb{P}$, there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

*Proof:* Consider $x^{p-1} - 1$ in $\mathbb{Z}_p[x]$. As $\mathbb{Z}_p$ is a field, this function has at most $p-1$ roots. By Fermat's little theorem, all of $1, 2, \ldots, p-1$ are the distinct roots. Now write $p = 4m+1$ for some $m \in \mathbb{N}$, so that

$$\begin{aligned} x^{p-1} - 1 &= x^{4m} - 1 \\ &= (x^4 - 1)(x^{4m-4} + x^{4m-8} + \cdots + x^4 + 1) \\ &= (x^2+1)(x-1)(x+1)(x^{4m-4} + x^{4m-8} + \cdots + x^4 + 1) \end{aligned}$$

Therefore $x^2 + 1$ has two unique roots, call them $c, d$. Hence $c^2 + 1 \equiv 0 \pmod p$, so write $c^2 + 1 = pk$ for some $k \in \mathbb{Z}$. As $c \in \{1, 2, \ldots, p-1\}$, we have that $pk < p^2$. Note that $p \mid c^2 + 1$, so if $p$ was prime over $\mathbb{Z}[i]$, then $p \mid c + i$ or $p \mid c - i$, but

$$v(p) = p^2 > pk = v(c+i) = v(c-i)$$

Hence $p \nmid c + i$ and $p \nmid c - i$, so $p$ is not prime over $\mathbb{Z}[i]$. As primes and irreducibles are equivalent in $\mathbb{Z}[i]$, we see that $p = (a+bi)(c+di)$, with $v(a+bi), v(c+di) > 1$. As $v(p) = p^2$, this implies that $v(a+bi) = p$, so $p = (a+bi)(a-bi)$, and $c = a, b = -d$. ■

**Remark 4.1.4.** This is a short summary of the properties of the Gaussian integers.

1. $1 + i$ is prime
2. $\pm 1, \pm i$ are units
3. If $p \equiv 3 \pmod 4$ is prime in $\mathbb{Z}$, then $p$ is prime in $\mathbb{Z}[i]$
4. If $p \equiv 1 \pmod 4$ is prime in $\mathbb{Z}$, then $a^2 + b^2 = p$ for $a, b \in \mathbb{Z}$, and $a + bi, a - bi$ are prime in $Z[i]$
5. There are no other primes

## 4.2 Algebraic extensions

**Definition 4.2.1.** Let $F$ be a subfield of a field $E$. Then $E$ is termed an extension (or extension field) of $F$.

**Example 4.2.2.**
- $\mathbb{C}, \mathbb{R}$ are extensions of $\mathbb{Q}$
- $\mathbb{Q}\langle\langle x\rangle\rangle$ is an extension of $\mathbb{Q}$
- $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is an extension of $\mathbb{Z}$

**Definition 4.2.3.** Let $E \ni \alpha$ be an extension of $F$. Then

$$\begin{aligned} F[\alpha] &= \{p(\alpha) \mid p(x) \in F[x]\} \\ F[\alpha_1, \ldots, \alpha_n] &= \{p(\alpha_1, \ldots, \alpha_n) \mid p(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]\} \\ F(\alpha) &= \left\{\tfrac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in F[x], g(\alpha) \neq 0\right\} \\ F(\alpha_1, \ldots, \alpha_n) &= \left\{\tfrac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n], g(\alpha_1, \ldots, \alpha_n) \neq 0\right\} \end{aligned}$$

**Remark 4.2.4.** $\mathbb{C}$ is an extension of $\mathbb{Q}$, with $\mathbb{Q}[i] = \mathbb{Q}(i)$, but $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$, as $\frac{1}{\pi} \notin \mathbb{Q}$.

**Definition 4.2.5.** Let $F, F'$ be fields. Then $\alpha \in F'$ is termed algebraic over $F$ iff there exists a non-zero polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$.

Then $f(x)$ is termed the minimal polynomial of $\alpha$ over $F$ iff $f(x)$ is monic and $g(\alpha) = 0$ for some $g(x) \in F[x]$ implies $\deg(g) \geqslant \deg(f)$. It follows immediately that the minimal polynomial is always irreducible.

**Theorem 4.2.6.** Let $E$ be an extension of $F$ with $\alpha \in E$. Let $p(x)$ be the minimal polynomial of $\alpha$. Then:
1. $F(\alpha) = F[\alpha] \approx F[x]/\langle p(x)\rangle$
2. $F(\alpha)$ is an $n$-dimensional vector space over $F$, with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$

*Proof:* **1.** Consider $\varphi : F[x] \to E$ given by $\varphi(f(x)) = f(\alpha)$, which is a homomorphism. Then $\varphi(F[x]) = F[\alpha]$, and by the 1st isomorphism theorem,

$$\varphi(F[x]) \approx F[x]/\ker(\varphi) = F[x]/\langle p(x)\rangle$$

Hence $F[\alpha] \approx F[x]/\langle p(x)\rangle$, and as $p(x)$ is irreducible, $F[x]/\langle p(x)\rangle$ is a field. Further, $F[\alpha] \subset F(\alpha)$, for $F(\alpha)$ the smallest field containing $\alpha$ and $F$. As $F[\alpha]$ is a field containing $\alpha$ and $F$, we have $F[\alpha] = F(\alpha)$. The result follows.

**2.** Let $V = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\}$, and we want to show that $V = F[\alpha]$. Let

$$\begin{aligned} p(x) &= x^n - b_{n-1}x^{n-1} - \cdots - b_1 x - b_0 \\ \implies \alpha^n &= b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 \in V \end{aligned}$$

Similarly, $\alpha^{n+1} = \alpha \cdot \alpha^n = b_{n-1}\alpha^n + \cdots + b_0\alpha \in V$, and so $\alpha^m \in V$ for all $m \in \mathbb{Z}_{\geqslant 0}$. Hence for all $f(x) \in F[x]$, we have that $f(\alpha) \in V$, and so $V = F[\alpha]$ as desired. ∎

**Definition 4.2.7.** Let $E$ be an extension of $F$. Then $E$ is termed a finite extension of $F$ iff $E$ can be expressed as a finite-dimensional vector space over $F$. If this dimension is $n$, then we write $[E : F] = n$. And $E$ is termed an algebraic extension of $F$ iff all $\alpha \in E$ are algebraic over $F$.

**Example 4.2.8.**
- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$
- $[\mathbb{C} : \mathbb{R}] = 2$, as $\mathbb{C} = \mathbb{R}[i]$, for $i^2 + 1 = 0$
- $\mathbb{R}, \mathbb{C}$ are extensions, but are neither algebraic nor finite extensions of $\mathbb{Q}$
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots)$ is an algebraic, but not a finite extension of $\mathbb{Q}$

**Theorem 4.2.9.** If $E$ is a finite extension of $F$, then $E$ is an algebraic extension of $F$.

*Proof:* Let $E$ be a finite extension of $F$, say $[E : F] = n$, and let $\beta \in E$. Consider the set $\{1, \beta, \beta^2, \ldots, \beta^n\}$, which must be linearly dependent in $E$. Hence there exists some $f(x) \in F[x]$ with $f(\beta) = 0$, and so $\beta$ is algebraic. Since $\beta$ was arbitrary, every element in $E$ is algebraic. ■

**Corollary 4.2.10.** Let $E$ be an extension of $F$. If $[E : F] = n$ and $\beta \in E$, then $\deg(\beta) \leqslant n$. Equivalently, $[F(\beta) : F] \leqslant [E : F]$.

**Theorem 4.2.11.** Let $K$ be a finite extension of $E$ and $E$ a finite extension of $F$. Then

$$[K : F] = [K : E][E : F]$$

*Proof:* As $E$ is a finite extension of $F$, say of dimension $n$, there exist $\alpha_1, \ldots, \alpha_n \in E$ with $E = \{\sum_{i=1}^n a_i\alpha_i \mid a_i \in F\}$. Similarly, $K = \{\sum_{i=1}^m b_i\beta_i \mid b_i \in E\}$ and $\beta_i \in K$. Hence we have that $\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_n\beta_m \in K$. We claim that

$$K = \left\{ \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij}\alpha_i\beta_j \mid c_{ij} \in F \right\}$$

It remains to be shown that if $\gamma \in K$, then $\gamma$ can be represented as an element in the set above, and that the set is minimal. So for $\gamma \in K$, we may express it as $\gamma = \sum_{j=1}^m b_j\beta_j$ for some $b_j \in E$. And as each $b_j \in E$, there exist $c_{ji} \in F$ such that $b_j = \sum_{i=1}^n c_{ji}\alpha_i$ for all $b_j$. Hence $\gamma$ has the required form.

Now suppose that

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij}\alpha_i\beta_j = \sum_{j=1}^{m} \underbrace{\left( \sum_{i=1}^{n} c_{ij}\alpha_i \right)}_{= b_j \in E} \beta_j$$

Then $\sum_{j=1}^m b_j\beta_j = 0$, and as $\beta_1, \ldots, \beta_m$ is a minimal set of vectors, it is linearly independent aver $E$. Hence $b_j = 0$ for all $j$. Then $\sum_{i=1}^n c_{ij}\alpha_i = 0$, and by a similar argument, $c_{ij} = 0$ for all $i$. Hence all the coefficients in the expression above are null, and the spanning set is minimal. ■

**Corollary 4.2.12.** Let $E$ be a finite extension of $F$, and $\alpha \in E$. Then $\deg(\alpha) = [F(\alpha) : F] \,\big|\, [E : F]$.

*Proof:* $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ ■

**Example 4.2.13.** For example, $\sqrt[3]{7} \notin \mathbb{Q}(\sqrt[4]{5})$.

**Corollary 4.2.14.** For $\alpha, \beta \in F$ algebraic, the elements $\alpha \pm \beta$, $\alpha \cdot \beta^{\pm 1}$ for $\beta \neq 0$ are all algebraic.

*Proof:* As $\alpha \pm \beta$, $\alpha \cdot \beta^{\pm 1} \in F(\alpha, \beta)$, WLOG assume that $[F(\alpha, \beta) : F(\alpha)] \leqslant [F(\alpha) : F]$. If $p(\beta) = 0$ for $p(x) \in F[x]$, then as $F[x] \subset F(\alpha)[x]$, $p(x) \in F(\alpha)[x]$. Hence $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F]$. ■

**Definition 4.2.15.** Let $\overline{\mathbb{Q}}$ be the set of algebraic numbers over $\mathbb{Q}$.

**Theorem 4.2.16.** Let $K$ be an algebraic extension of $E$, and $E$ an algebraic extension of $F$. Then $K$ is an algebraic extension of $F$.

*Proof:* Let $\gamma \in K$, so $\gamma$ is the root of $p(x) = \sum_{i=1}^n a_i x^i$, for $a_i \in E$. As all $a_i \in E$ are algebraic, we have that $[F(a_i) : F] \leqslant \deg(a_i) = m_i < \infty$. Let $L = F(a_1, \ldots, a_n)$, and note that $\gamma \in L(\gamma) \subset K$. Further,

$$[L(\gamma) : F] = \underbrace{[L(\gamma) : L]}_{\leqslant\ n} \underbrace{[L : F]}_{= \prod m_i}$$

Hence $L(\gamma)$ is a finite extension of $F$, and so it is an algebraic extension, so $\gamma$ is algebraic in $L(\gamma)$. Then $\gamma$ is algebraic in $K$, and $K$ is an algebraic extension of $F$. ■

## 4.3 Splitting fields

**Definition 4.3.1.** Given a field $E$, a polynomial $p(x)$ is said to split over $E$ if

$$p(x) = a\prod_{i=1}^{n}(x-\alpha_i), \qquad \alpha_i \in E$$

**Definition 4.3.2.** Given a polynomial $p(x) \in F[x]$, an extension field $K$ of $F$ is termed a splitting field of $p(x)$ iff $p(x)$ splits over $K$, and $K$ is the smallest such field (smallest by inclusion).

**Example 4.3.3.** Find the splitting field for $p(x) = x^4 - 4 \in \mathbb{Q}[x]$.

Note that

$$\begin{aligned} p(x) = (x^2-2)(x^2+2) &= (x+\sqrt{2})(x-\sqrt{2})(x^2+2) \in \mathbb{Q}(\sqrt{2}) \\ &= (x^2-2)(x+\sqrt{2}i)(x-\sqrt{2}i) \in \mathbb{Q}(\sqrt{2}i) = \mathbb{Q}(\sqrt{-2}) \end{aligned}$$

So we choose $p(x) = (x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{2}i)(x-\sqrt{2}i) \in \mathbb{Q}(\sqrt{2}, i)$.

**Theorem 4.3.4.** Let $f(x) \in F[x]$ split over $E$ as $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$. Then the splitting field of $f(x)$ is $F(\alpha_1, \ldots, \alpha_n)$.

**Theorem 4.3.5.** Let $f(x) \in F[x]$ be of degree $n$. Then the splitting field of $f(x)$, say $E$, satisfies $[E:F] \leqslant n!$

*Proof:* Let $\alpha_1$ be a root of $f(x)$. Then there exists $f_{n-1} \in F(\alpha_1)$ of degree $n-1$ such that $[F(\alpha_1):F] \leqslant n$ with $f(x) = (x-\alpha_1)f_{n-1}(x)$.

Pick a root $\alpha_2$ of $f_{n-1}(x)$ and repeat the process with $f_{n-2} \in F(\alpha_1, \alpha_2)$ of degree $n-2$ such that $[F(\alpha_1,\alpha_2) : F(\alpha_1)] \leqslant n-1$ with $f_{n-1}(x) = (x-\alpha_2)f_{n-2}(x)$.

Repeat this process as necessary, to get ultimately that

$$\begin{aligned} [F(\alpha_1,\ldots,\alpha_n):F] &= [F(\alpha_1,\ldots,\alpha_n) : F(\alpha_1,\ldots,\alpha_{n-1}][F(\alpha_1,\ldots,\alpha_{n-1}) : F(\alpha_1,\ldots,\alpha_{n-2})]\cdots[F(\alpha_1):F] \\ &\leqslant 1\cdot 2\cdots n \\ &= n! \end{aligned}$$

■

**Example 4.3.6.** Find the splitting field for $x^3 - 2$ over $\mathbb{Q}$.

Pick the first root $\alpha_1 = 2^{1/3}$, so in $\mathbb{Q}(2^{1/3})$, $f(x) = (x-2^{1/3})(x^2+2^{1/3}x+2^{2/3})$, and $[\mathbb{Q}(2^{1/3}):\mathbb{Q}] = 3$. Let $\omega = \frac{-1+\sqrt{3}}{2}$ be the non-trivial cube root of unity. Then

$$f(x) = (x-2^{1/3})(x-2^{1/3}\omega)(x-2^{1/3}\omega^2)$$

Moreover, $[F(2^{1/3}, 2^{1/3}\omega) : F(2^{1/3})] = 2$, and so $[F(2^{1/3}, 2^{1/3}\omega) : F] = 2\cdot 3 = 6$, and $F(2^{1/3}, 2^{1/3}\omega)$ is the splitting field.

**Remark 4.3.7.** If $\alpha_1, \ldots, \alpha_k$ are all algebraic over $\mathbb{Q}$, then there exists $\beta$ algebraic over $\mathbb{Q}$ with $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, however it is very difficult to calculate $\beta$ explicitly. This holds in general for any field $F$, not just $\mathbb{Q}$.

## 4.4 Finite fields

**Example 4.4.1.** These are some examples of finite fields:

- $\mathbb{Z}_p$ for $p$ prime
- $\mathbb{Z}_p[x]/\langle f(x)\rangle$ for $f$ irreducible

**Theorem 4.4.2.** Let $F$ be a finite field. Then there exists a prime $p$ and an integer $n \geqslant 1$ such that:
- $F$ has characteristic $p$
- $F$ has $p^n$ elements

*Proof:* As $F$ is a field, it is an integral domain. As $F$ is a finite integral domain, we know from the midterm that $\text{char}(F) = p$ for some prime $p$. For '1' the unit of $F$, define

$$E = \{n \cdot \text{`1'} \mid n \in \mathbb{Z}\} \subset F$$

Note that $E \approx \mathbb{Z}_p$, which is a field. So $F$ is an extension field of $E$.

If $F = E$, then we are done. Else pick $\alpha_2 \in F \setminus E$ and write

$$E_2 = \{a_1 + a_2\alpha_2 \mid a_i \in E\}$$

Note that $E_2$ is not necessarily a field, it is just a vector space over $E$.

If $F = E_2$, then we are done. Else repeat the above with some $\alpha_3 \in F \setminus E_2$ and

$$E_3 = \{a_1 + a_2\alpha_2 + a_3\alpha_3 \mid a_i \in E\}$$

At some point this process must stop, as $F$ is finite. So say this process stops at $F = E_n$. Note that $E_n$ has $p^n$ elements, so $F$ does too. ■

**Theorem 4.4.3.** If $F$ is a field with $p^n$ elements, then $F$ is isomorphic to the splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$. Furthermore, the splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$ has $p^n$ elements.

*Proof:* Let $F$ be the field with $p^n$ elements, and $k = p^n - 1$. Let $a_1, \ldots, a_k$ be the non-zero elements in $F$, and write $u = a_1 a_2 \cdots a_k$. Note that the map $x \mapsto cx$ for any nonzero $c$ is an automorphism of $\{a_1, \ldots, a_k\}$, so it is a bijection. This implies that

$$u = (ca_1)(ca_2)\cdots(ca_k) = c^k a_1 a_2 \cdots a_k = c^k u$$

Hence $c^{p^n-1} = 1$ for nonzero $c$, so $c^{p^n} = c$ for all $c$. Hence for every $c \in F$, $c^{p^n} - c = 0$. As there are $p^n$ elements in $F$,

$$x^{p^n} - x = \prod_{c \in F} (x - c)$$

To complete the proof, it must be shown that if $a, b$ satisfy $a^{p^n} - a = b^{p^n} - b = 0$, then so do $a + b, ab$ and $a^{-1}$. This follows from simple calculations.

$$\begin{aligned}(ab)^{p^n} &= a^{p^n} b^{p^n} = ab \\ (a+p)^{p^n} &= a^{p^n} + b^{p^n} = a + b \\ (a^{-1})^{p^n} &= (a^{p^n-2})^{p^n} = (a^{p^n})^{p^n-2} = a^{p^n-2} = a^{-1}\end{aligned}$$

Hence $F$ is the splitting field of $x^{p^n} - x$ and has $p^n$ elements. ■

Note that the set of roots of $x^{p^n} - x$ forms a field.

**Corollary 4.4.4.** Let $f(x) \in \mathbb{Z}_p[x]$ be irreducible for $p$ prime. Then $\mathbb{Z}_p[x]/\langle f(x)\rangle \approx$ (splitting field of $x^{p^n} - x$).

For instance, we have that $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle \approx \mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$.

**Corollary 4.4.5.** If $f(x) \in \mathbb{Z}_p[x]$ has an irreducible factor of degree $n$, then $\gcd(f(x), x^{p^n} - x) \neq 1$.

**Definition 4.4.6.** The Galois field of $p^n$ elements is defined as $GF(p^n) =$(splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$).

**Remark 4.4.7.** All finite fields are $GF(p^n)$ for some $p$ and $n$.

**Example 4.4.8.** Explicitly calculate $GF(2^6)$ and all its subfields.

We first claim that $f(x) = x^6 + x^3 + 1$ is irreducible.

To see it has no linear factors, note $f(0) = f(1) = 1 \neq 0$

To see it has no quadratic factors, note

$$\begin{aligned}\gcd(x^6 + x^3 + 1, x^{2^2} - x) &= \gcd(x^6 + x^3 + 1, x^4 - x) \\ &= \gcd(x^6 + x^3 + 1 - x^2(x^4 + x), x^4 + x) \\ &= \gcd(1, x^4 - x) \\ &= 1\end{aligned}$$

To see it has no cubic factors, note

$$\begin{aligned}\gcd(x^6 + x^3 + 1, x^{2^3} - x) &= \gcd(x^6 + x^3 + 1, x^8 - x) \\ &= \gcd(x^6 + x^3 + 1, x^5 + x^2 + x) \\ &= \gcd(x^2 + 1, x^5 + x^2 + x) \\ &= \gcd(x^2 + 1, x^3 + x^2 + x) \\ &= \gcd(x^2 + 1, x^2) \\ &= \gcd(1, x^2) \\ &= 1\end{aligned}$$

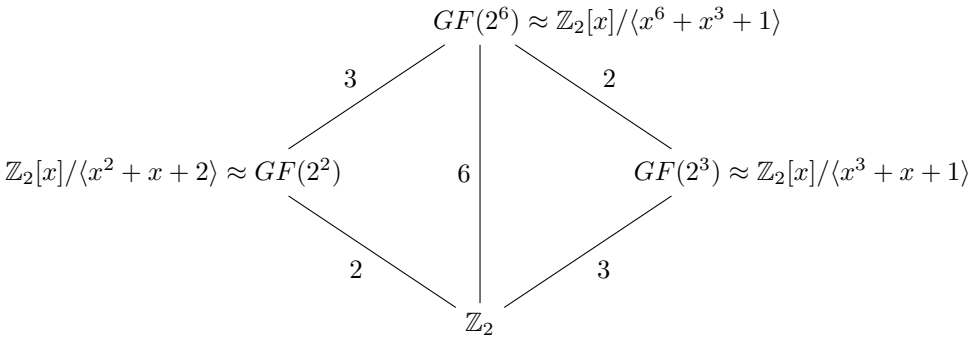
Hence it is irreducible, and $GF(2^6) \approx \mathbb{Z}_2[x]/\langle x^6 + x^3 + 1\rangle$. Now to find the subfields, first note that as $[GF(2^6) : \mathbb{Z}_2] = 6$, for $F$ a subfield with $[GF(2^6) : F][F : \mathbb{Z}_2]$, we can have $[F : \mathbb{Z}_2] \in \{1, 2, 3, 6\}$.

If $[F : \mathbb{Z}_2] = 1$, then $F = \mathbb{Z}_2$
If $[F : \mathbb{Z}_2] = 2$, then $F = GF(2^2)$
If $[F : \mathbb{Z}_2] = 3$, then $F = GF(2^3)$
If $[F : \mathbb{Z}_2] = 6$, then $F = GF(2^6)$

To see that the above holds for $2, 3$, note that for $\alpha \in GF(2^2)$ and $\beta \in GF(2^3)$, we have

$$\begin{aligned}\alpha^{64} &= (\alpha^4)^{16} = \alpha^{16} = (\alpha^4)^4 = \alpha^4 = \alpha \\ \beta^{64} &= (\beta^8)^8 = \beta^8 = \beta\end{aligned}$$

Hence $\alpha, \beta \in GF(2^6)$, giving a construction as follows:




Note that $x^6 + x^3 + 1$ is not irreducible in $GF(2^3)$ or $GF(2^2)$, as if it was, then the degree of the extension would be 6, instead of 3 and 2 as shown above.

**Definition 4.4.9.** Let $R$ be a ring. A map $\sigma : R \to R$ is termed an automorphism from $R$ to itself iff it is a bijective ring homomorphism. The group (it wil be shown below to be a group) of automorphisms on $R$ is denoted by $\mathsf{Aut}(R)$.

For exapmle, the map $\sigma(a) = a$ is termed the trivial automorphism.

**Definition 4.4.10.** Let $F$ be a finite field of characteristic $p$. Then the map $\varphi : F \to F$ given by $a \mapsto a^p$ is termed the Frobenius map.

**Proposition 4.4.11.** The Frobenius map is an automorphism.

*Proof:* First check that it is a ring homomorphism.

$$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$

To see that it is injective, if $\varphi(a) = \varphi(b)$, then

$$a^p = b^p \implies a^p - b^p = 0 \implies (a-b)^p = 0 \implies a - b = 0 \implies a = b$$

As $F$ is finite and $\varphi$ in injective, surjectivity follows. ■

**Example 4.4.12.** Factor $x^6 + x^3 + 1$ over $GF(2^3)$.

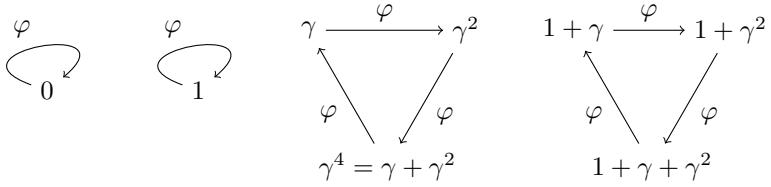
Suppose that for some $\alpha, \beta$, $x^2 + \alpha x + \beta | x^6 + x^3 + 1$ in $GF(8)[x]$. Now apply the Frobenius map:

$$(1)^2 x^2 + \alpha^2 x + \beta^2 | x^6 + x^3 + 1$$
$$(1)^4 x^2 + \alpha^4 x + \beta^4 | x^6 + x^3 + 1$$

If one of the factors above splits, then all of them do, hence they would all be irreducible. Assuming $\alpha^2 \neq \alpha$ and $\beta^2 \neq \beta$, they are all distinct factors. Therefore

$$x^6 + x^3 + 1 = (x^2 + \alpha x + \beta)(x^2 + \alpha^2 x + \beta^2)(x^2 + \alpha^4 x + \beta^4)$$

in $GF(8)[x]$. As $GF(2^3) \approx \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ from above, consider $\gamma$ as the root of $x^3 + x + 1$, where $GF(8) = \{a + b\gamma + c\gamma^2 \mid a, b, c \in \mathbb{Z}_2, \gamma^3 = \gamma + 1\}$. Then consider the action of the Frobeinus map $\varphi$ on the elements of $GF(8)$.




So let $\alpha = a\gamma^2 + b\gamma + c$ and $\beta = d\gamma^2 + e\gamma + f$, and rewrite $x^6 + x^3 + 1$ in terms of $\gamma$. By simplifying, we find

$$\begin{array}{ll} a = 1 & d = 0 \\ b = 0 & e = 0 \\ c = 0 & f = 1 \end{array}$$

Hence the expression $x^6 + x^3 + 1$ may be expressed as

$$x^6 + x^3 + 1 = (x^2 + \gamma^2 x + 1)(x^2 + (\gamma^2 + \gamma)x + 1)(x^2 + \gamma x + 1)$$

# 5 Galois theory

## 5.1 Introduction

**Definition 5.1.1.** A group is a set $G$ with a binary operation (usually $+$ or $\cdot$, but $*$ in general) such that for $a, b, c \in G$,

1. $ab \in G$
2. there exists $e \in G$ such that $ae = ea = a$
3. there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$
4. $a(bc) = (ab)c$

Frequently the group is denoted $(G, *)$.

**Example 5.1.2.**
· A ring with the binary operation $+$ is a group, with $e = 0$
· The non-zero elements in a division ring under $\cdot$ form a group, with $e = 1$
· The set of permutations under composition form a group, called $S_3$ (this generalizes to $S_n$)

**Example 5.1.3.** Find the set of all automorphisms of $\mathbb{Q}(\sqrt{2})$.

Let $\varphi$ be an automorphism, so $\varphi(1) = 1$, and $\varphi(a) = \underbrace{1 + 1 + \cdots + 1}_{a \text{ times}} = a$ for all $a \in \mathbb{Q}$. Moreover, then $\varphi(a + b\sqrt{2}) = a + b\varphi(\sqrt{2})$, hence $\varphi$ is determined completely by what it does to $\sqrt{2}$.

Note that $\varphi(\sqrt{2})\varphi(\sqrt{2}) = \varphi(2) = 2$, so $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Let $\varphi^+(\sqrt{2}) = \sqrt{2}$ and $\varphi^-(\sqrt{2}) = -\sqrt{2}$. Then the group table is given by

| $\circ$ | $\varphi^+$ | $\varphi^-$ |
|---|---|---|
| $\varphi^+$ | $\varphi^+$ | $\varphi^-$ |
| $\varphi^-$ | $\varphi^-$ | $\varphi^+$ |

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

Therefore the set of all automorphisms of $\mathbb{Q}(\sqrt{2})$ is isomorphic to $\mathbb{Z}_2$.

**Definition 5.1.4.** Let $E$ be an extension field of $F$. Then $\gamma \in \mathsf{Aut}(E)$ is termed an $F$-automorphism iff $\gamma(a) = a$ for all $a \in F$.

**Example 5.1.5.** The automorphisms of $\mathbb{Q}(\sqrt{5})$ are $\sigma_\pm(a + b\sqrt{5}) = a \pm b\sqrt{5}$.

Here we have that $\sigma_+$ is both a $\mathbb{Q}(\sqrt{5})$- and $\mathbb{Q}$-automorphism, whereas $\sigma_-$ is only a $\mathbb{Q}$-automorphism.

**Definition 5.1.6.** Let $G$ be a group. A set $H \subset G$ is termed a subgroup of $G$ iff $H$ is a group under the same binary operation as $G$. This relationship is denoted $H \leqslant G$.

## 5.2 The group $\mathsf{Gal}(E/F)$

**Definition 5.2.1.** Let $E$ be an extension field of $F$. Then the Galois group $\mathsf{Gal}(E/F)$ is the group of $F$-automorphisms of $E$.

**Theorem 5.2.2.** Let $E$ be an extension of $F$. Then
1. $(\mathsf{Aut}(E), \circ)$ is a group
2. The set of $F$-automorphisms as a subset of $\mathsf{Aut}(E)$ is a subgroup of $\mathsf{Aut}(E)$

*Proof:* **1.** Let $\sigma, \tau \in \mathsf{Aut}(E)$. We need to show that $\sigma \circ \tau \in \mathsf{Aut}(E)$. Note

$$\begin{aligned} \sigma \circ \tau(a + b) &= \sigma(\tau(a + b)) \\ &= \sigma(\tau(a) + \tau(b)) \\ &= \sigma(\tau(a)) + \sigma(\tau(b)) \\ &= \sigma \circ \tau(a) + \sigma \circ \tau(b) \end{aligned} \qquad \begin{aligned} \sigma \circ \tau(ab) &= \sigma(\tau(ab)) \\ &= \sigma(\tau(a)\tau(b)) \\ &\sigma(\tau(a))\sigma(\tau(b)) \\ &= \sigma \circ \tau(a) \cdot \sigma \circ \tau(b) \end{aligned}$$

Hence it is a homomrphism. As both $\sigma, \tau$ are bijections, their composition is a bijection, and so $\sigma \circ \tau \in \mathsf{Aut}(E)$.

For $\mathsf{Id}(a) = a$ the identity automorphism, clearly $\mathsf{Id} \in \mathsf{Aut}(E)$ is the identity element.

As $\sigma \in \mathsf{Aut}(E)$ is bijective, also $\sigma^{-1} \in \mathsf{Aut}(E)$ and $\sigma^{-1} \circ \sigma = \mathsf{Id}$.

Standard composition of functions gives that $\sigma \circ (\tau \circ \theta) = (\sigma \circ \tau) \circ \theta$.

Hence $\mathsf{Aut}(E)$ is a group.

The fact that $\mathsf{Gal}(E/F)$ is a subgroup is done identicaly. ■

**Theorem 5.2.3.** Let $\alpha$ be algebraic over $F$ and $\sigma \in \mathsf{Gal}(E/F)$. For $p(x)$ the minimal polynomial of $\alpha$, $\sigma(\alpha)$ is a root of $p$.

*Proof:*

$$\begin{aligned} p(\alpha) &= a_n\alpha^n + \cdots + a_0 = 0 \\ \sigma(p(\alpha)) &= \sigma(a_n\alpha^n + \cdots + a_0) \\ &= \sigma(a_n\alpha^n) + \cdots + \sigma(a_0) \\ &= a_n\sigma(\alpha^n) + \cdots + a_0 \\ &= a_n\sigma(\alpha)^n + \cdots + a_0 \\ &= p(\sigma(\alpha)) \end{aligned}$$

Therefore $\sigma(p(\alpha)) = p(\sigma(\alpha)) = 0$. ■

**Example 5.2.4.** Find $\mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.

Note that as $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ and for $\sigma \in \mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, we have $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$ for $\omega^2+\omega+1 = 0$, or $\omega$ the third root of unity.

However, note that $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \notin \mathbb{Q}(\sqrt[3]{2})$, hence $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Hence $\mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \approx \mathbb{Z}_1$, the trivial group of size 1.

**Theorem 5.2.5.** Let $\alpha$ be algebraic over $F$. Then $\sigma \in \mathsf{Gal}(F(\alpha)/F)$ is completely determined by $\sigma(\alpha)$.

**Corollary 5.2.6.** $|\mathsf{Gal}(F(\alpha)/F)| \leqslant \deg_F(\alpha)$

**Example 5.2.7.** Find $|\mathsf{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})|$.

The minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$, which factors as $(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x + \sqrt{2})$ over $\mathbb{Q}(\sqrt[4]{2})$. Hence for $\sigma \in \mathsf{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$, we have that $\sigma(\sqrt[4]{2}) = \pm\sqrt[4]{2}$, and so $|\mathsf{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})| = 2 \leqslant 4$.

**Corollary 5.2.8.**

$$|\mathsf{Gal}(F(\alpha_1, \ldots, \alpha_n)/F)| \leqslant \prod_{i=1}^{n} \deg_F(\alpha_i)$$

**Example 5.2.9.** Let $E$ be the splitting field of $x^3 - 2$. Find $\mathsf{Gal}(E/\mathbb{Q})$.

Here, $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$, for $\omega^2 + \omega + 1 = 0$. If $\varphi \in \mathsf{Gal}(E/\mathbb{Q})$, then

$$\begin{aligned} \varphi(\sqrt[3]{2}) &\in \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\} \\ \varphi(\omega) = \varphi\left(\tfrac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}\right) &\in \{\omega, \omega^2\} \end{aligned}$$

The second statement follows as $\frac{1}{\omega} = \omega^2$ and $\frac{1}{\omega^2} = \omega$. Therefore specifying these two actions will completely determine the automorphism. Hence $\mathsf{Gal}(E/Q)$ is a group with 6 elements.

As any one of $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ can be mapped to any other one in that list, it follows that the group is isomorphic to $S_3$.

**Theorem 5.2.10.** Let $F \approx F'$ via $\varphi : F \to F'$. Let $p(x) \in F[x]$ be irreducible. Then $p'(x) = \varphi(p(x)) \in F'[x]$ is irreducible. Further, $F[x]/\langle p(x)\rangle \approx F'[x]/\langle p'(x)\rangle$ by $\varphi(q(x) + \langle p(x)\rangle) = \varphi(q(x)) + \langle p'(x)\rangle$.

**Example 5.2.11.** Consider the sequence of splitting fields for the splitting field of $x^4 - 2$.

First, use $F = F' = \mathbb{Q}$, and $p(x) = p'(x) = x^4 - 2$. This gives a homomorphism $\varphi(\sqrt[4]{2}) = \sqrt[4]{2}i$.

Next, use $F = \mathbb{Q}(\sqrt[4]{2})$ and $F' = \mathbb{Q}(\sqrt[4]{2}i)$, with $p(x) = x^2 + \sqrt{2}$ and $p'(x) = x^2 - \sqrt{2}$.

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i) \approx \mathbb{Q}(\sqrt[4]{2})[x]/\langle x^2 + \sqrt{2}\rangle & & \mathbb{Q}(\sqrt[4]{2}i)[x]/\langle x^2 - \sqrt{2}\rangle \approx \mathbb{Q}(\sqrt[4]{2}i, \sqrt[4]{2}) \\ \diagdown & & \diagup \\ \mathbb{Q}(\sqrt[4]{2}) \approx \mathbb{Q}[x]/\langle x^4 - 2\rangle & & \mathbb{Q}[x]/\langle x^4 - 2\rangle \approx \mathbb{Q}(\sqrt[4]{2}i) \\ & \diagdown \quad \diagup & \\ & \mathbb{Q} & \end{array}$$

Now we have that $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i)$ is isomorphic to itself, but the isomorphism constructed here gives $\sqrt[4]{2} \mapsto \sqrt[4]{2}i$.

**Proposition 5.2.12.** Let $E$ be the splitting field of an irreducible polynomial $p(x)$ over $F$. Then for all pairs of roots $\alpha, \beta$ of $p(x)$, there exists $\sigma \in \mathsf{Gal}(E/F)$ with $\sigma(\alpha) = \beta$.

**Remark 5.2.13.** We do not need for $E$ to be the splitting field of $p(x)$. We only need $p(x)$ to split in $E$.

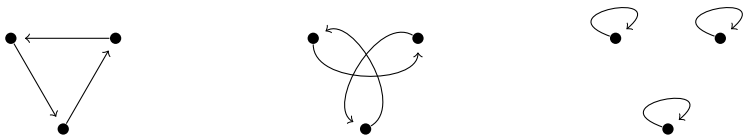
In particular, recall from a previous example that there were $\sigma, \theta \in \mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ such that $\sigma(\sqrt[3]{2}) =$ any root of $x^3 - 2$, and $\theta(\omega) = \omega$ or $\omega^2$. Now consider the following:

$$\begin{aligned} \sigma(\sqrt[3]{2}) &= \sqrt[3]{2}\omega \\ \sigma(\sqrt[3]{2}\omega) &= \sqrt[3]{2}\omega^2 \\ \sigma(\sqrt[3]{2}\omega^2) &= \sqrt[3]{2} \end{aligned}$$

Further, observe that

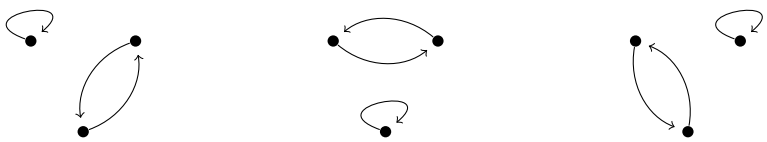
$$\sigma\left(\frac{1}{\omega}\right) = \sigma\left(\frac{\sqrt[3]{2}}{\sqrt[3]{2}\omega}\right) = \frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}\omega^2} = \frac{1}{\omega}$$

Hence $\sigma(\omega) = \omega$ and $\sigma(\omega^2) = \omega^2$. Hence we have the transformations of $\sigma, \sigma^2$, and $\sigma^3$ represented by



$\sigma$ $\qquad$ $\sigma^2$ $\qquad$ $\sigma^3$

Note not all possible maps are represented above, as there is $\theta$ with $\theta(\omega) = \omega^2$, but $\sigma^n(\omega) = \omega$ for all $n$. For $\theta(\omega) = \omega$, we have that $\theta \circ \sigma^n = \sigma^n$ for $n = 1, 2, 3$. The other three maps are given by applying $\theta$ to each of the maps above, for $\theta(\omega) = \omega^2$.



$\theta \circ \sigma$ $\qquad$ $\theta \circ \sigma^2$ $\qquad$ $\theta \circ \sigma^3$

**Definition 5.2.14.** A polynomial $f(x) \in F[x]$ is termed separable over $F$ iff the roots of $f(x)$ over its splitting field have multiplicity 1.

**Remark 5.2.15.** Let $F$ be a field of characteristic 0. Then any irreducible polynomial in $F[x]$ is separable.

**Theorem 5.2.16.** Let $F$ be a field with non-zero characteristic with $p(x) \in F[x]$ irreducible. If $\gcd(p(x), p'(x)) = 1$, then $p(x)$ is separable.

If $p(x)$ is irreducible and not separable, then $p'(x) = 0$, or equivalently, $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

**Definition 5.2.17.** Let $E$ be an extension field of $F$. Then $\alpha \in F$ is termed separable iff the minimal polynomial of $\alpha$ in $F[x]$ is separable.

Then $E$ is termed a separable extension of $F$ iff all $\alpha \in E$ are separable.

Then $F$ is termed perfect iff all algebraic extensions of $F$ are separable extensions.

**Example 5.2.18.** The fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, GF(p^n)$ are all perfect, for $p$ prime and $n \in \mathbb{N}$.

**Theorem 5.2.19.** Let $f(x) \in F[x]$ be separable, and $E$ be the splitting field of $f(x)$. Then $|\mathsf{Gal}(E/F)| = [E : F]$.

*Proof:* This proof will proceed by induction. Clearly the theorem holds for $[E : F] = 1$, so suppose that it holds for $[E : F] = m$, for all $m < n$.

Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with roots $\alpha_1, \ldots, \alpha_k$, where $k \leqslant n$. By a previous theorem, there exist maps $\theta_1, \ldots, \theta_k \in \mathsf{Gal}(E/F)$ with $\theta_i(\alpha_1) = \alpha_i$.

As $E$ is a splitting field over $F$, it is a splitting field over $F(\alpha_1)$. Note that $[E : F(\alpha_1)] < n$, as $[E : F] = [E : F(\alpha_1)]\underbrace{[F(\alpha_1) : F]}_{k \geqslant 2}$, and so $[E : F(\alpha_1)] = m = n/k$, and by induction, $[E : F(\alpha_1)] = |\mathsf{Gal}(E/F(\alpha_1))|$.

Let $\psi_1, \ldots, \psi_m \in \mathsf{Gal}(E/F(\alpha_1))$ be an exhaustive, distinct list. Now we claim that the desired set of automorphisms is $\{\theta_1 \circ \psi_1, \theta_1 \circ \psi_2, \ldots, \theta_k \circ \psi_m\} = \mathsf{Gal}(E/F)$. It must be shown that they are distinct and exhaustive.

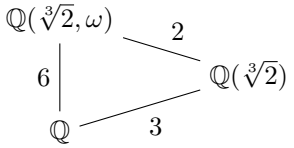
To see that they are all distinct, note that $\theta_i \circ \psi_j(\alpha_1) = \theta_i(\alpha_1) = \alpha_i$, and that $\theta_i \circ \psi_j = \theta_w \circ \psi_z$ implies $i = w$. Then $\psi_j = \psi_z$, so $j = z$, and hence they are all distinct.

Now suppose that $\sigma \in \mathsf{Gal}(E/F)$, hence $\sigma(\alpha_1) = \alpha_s$ for some $s \in [1, m]$. Note that $\theta_s^{-1} \circ \sigma(\alpha_1) = \theta_s^{-1}(\alpha_s) = \alpha_1$, so $\sigma(\alpha_1) = \theta_s(\alpha_1)$. Therefore $\theta_s^{-1} \circ \sigma$ fixes $F(\alpha_1)$ and $\theta_s^{-1} \circ \sigma \in \mathsf{Gal}(E/F(\alpha_1))$, and so

$$\theta_s^{-1} \circ \sigma = \psi_j \implies \sigma = \theta_s \circ \psi_j$$

Hence $\sigma$ is one of the described forms, and $|\mathsf{Gal}(E/F)| = [E : F] = mk$. ■

**Example 5.2.20.** Let $E$ be the splitting field of $x^3 - 2$, so then




Hence $\mathsf{Gal}(E/\mathbb{Q})$ has size 6.

**Theorem 5.2.21.** Let $E$ be a splitting field of a separable polynomial of degree $n$ over $F$. Then

$$\mathsf{Gal}(E/F) \leqslant S_n \qquad \text{and so} \qquad |\mathsf{Gal}(E/F)| \leqslant n!$$

*Proof:* The set of permutations of all roots of $f(x)$ contains $\mathsf{Gal}(E/F)$ as a subgroup, and the set of permutations of $n$ elements is isomorphic to $S_n$. The size follows from a theorem of Lagrange. ■

**Definition 5.2.22.** Let $E$ be a finite extension of $F$. Then $E$ is termed primitive, or a simple extension iff there exists $\gamma \in E$ with $E = F(\gamma)$.

**Example 5.2.23.**
- The field $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ for distinct primes $p, q$ is a simple extension, as $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$
- The field $GF(2^2)$ is a simple extension of $\mathbb{Z}_2$

**Theorem 5.2.24.** Let $E$ be a finite separable extension of $F$. Then $E$ is a simple extension of $F$.

*Proof:* Case 1: $F$ is finite.
As $F$ is a finite field, $F \approx GF(p^n)$ for some $p, n$. As $E$ is a finite extension, $E \approx GF(p^m)$ for $m \geqslant n$. We know that $E \approx \mathbb{Z}_p[x]/\langle f(x) \rangle$ for $f(x) \in \mathbb{Z}_p[x]$ an irreducible polynomial of degree $m$. Let $\alpha$ be a root of $f$, so $E = F(\alpha)$.

Case 2: $F$ is infinite.
As $E$ is a finite extension, $E = F(\alpha_1, \ldots, \alpha_n)$, and we wish to show that there exists a $\gamma$ with $E = F(\gamma)$. It suffices to show that $E = F(\alpha_1, \alpha_2)$ and there is a $\gamma$ with $E = F(\gamma)$, as

$$F(\alpha_1, \ldots, \alpha_n) = F(\gamma_1, \alpha_3, \ldots, \alpha_n) = F(\gamma_2, \alpha_4, \ldots, \alpha_n)$$

for appropriate $\gamma_i$. Now assume that $E = F(\alpha, \beta)$. Let $f, g$ be the minimal polynomials of $\alpha, \beta$ over $F[x]$. Let $E_2$ be the splitting field of $f, g$, so both factor completely over $E_2[x]$. Let $a_1, \ldots, a_n$ be the roots of $f$, and $b_1, \ldots, b_k$ be the roots of $g$, where $\prod a_i = \alpha$ and $\prod b_i = \beta$. Also note that all $b_i$ are distinct. Pick

$$u \in F,\ u \neq \frac{a_1 - a_i}{b_1 - b_j}\ \ \forall\, i = 1, \ldots, n\ \ \forall\, j = 1, \ldots, k$$

As $F$ is infinite, there are lots of choices for $u$. Define

$$\gamma = a_1 + ub_1 = \alpha + u\beta$$

We claim that $F(\gamma) = F(\alpha, \beta)$. As $\gamma \in F(\alpha, \beta)$, we have that $F(\gamma) \subset F(\alpha, \beta)$. If we can show that $\beta \in F(\gamma)$, then as $\alpha = \gamma - u\beta$, we will be done.

Let $h(x)$ be the minimal polynomial of $\beta$ in $F(\gamma)$. If $\deg(h) = 1$, then we are done. Note that

$$g(x) = (x - b_1)(x - b_2) \ldots (x - b_k) \in F[x] \subset F(\gamma)$$

Hence $h(x) \mid g(x)$. Let $k(x) = f(\gamma - ux) \in F(\gamma)[x]$. Further,

$$k(b_1) = f(\gamma - ub_1) = f(\alpha + u\beta - u\beta) = p(\alpha) = 0$$

Hence $\beta$ is a root of $k(x)$.

So $h(x) \mid k(x)$ and $h(x) \mid \gcd(g(x), k(x))$. Note that the roots of $g(x)$ are $b_1, \ldots, b_k$. If we can show that $k(b_j) \neq 0$ for all $j = 2, \ldots, k$, then the only factor in common is $x - \beta$, so $h(x) = x - \beta$, and $\beta \in F(\gamma)$. Now

obsorve that

$$\begin{aligned} k(b_j) &= p(\gamma - ub_j) \\ &= \prod_i ((\gamma - ub_j) - a_i) \\ &= \prod_i (a_1 + ub_1 - ub_j - a_i) \\ &= \prod_i (a_1 - a_i - u(b_1 - b_j)) \\ &= \prod_i \left( \underbrace{\left( \frac{a_1 - a_i}{b_1 - b_j} - u \right)}_{\neq 0} (b_1 - b_j) \right) \end{aligned}$$

Therefore $\gcd(k(x), g(x)) = x - \beta$, so $\beta \in F(\gamma)$ and $F(\gamma) = F(\alpha, \beta)$. ■

**Example 5.2.25.** Construct $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ as a simple extension of $\mathbb{Q}$.

Now, we already know that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{5})$. Further, let

$$u = 1 \neq \frac{\sqrt{2} \pm \sqrt{2}}{\sqrt{3} - (-\sqrt{3})}$$

The minimal polynomial of $\sqrt{2} + \sqrt{3}$ is

$$p(x) = (x - (\sqrt{2} + \sqrt{3}))(x - (\sqrt{2} - \sqrt{3}))(x - (-\sqrt{2} + \sqrt{3}))(x - (-\sqrt{2} - \sqrt{3}))$$

Again we can take

$$u = 1 \neq \frac{\sqrt{2} + \sqrt{3} \pm \sqrt{2} \pm \sqrt{3}}{\sqrt{5} - (-\sqrt{5})}$$

Hence $Q(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$.

## 5.3 The fundamental theorem of Galois theory

**Theorem 5.3.1.** Let $F \subset K \subset E$ be a sequence of extensions. Then $\mathsf{Gal}(E/K) \leqslant \mathsf{Gal}(E/F)$.

*Proof:* If $\sigma \in \mathsf{Gal}(E/K)$, then $\sigma$ is an automorphism of $E$ that fixes $K$ (and hence $F$). So $\sigma \in \mathsf{Gal}(E/F)$. Further, $\mathsf{Gal}(E/K)$ is a group, and as it is contained in another group, it must be a subgroup. ■

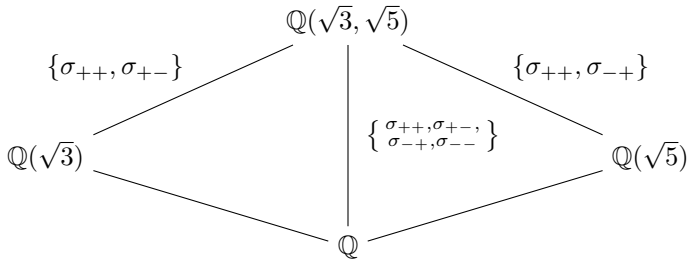
**Example 5.3.2.** Recall that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Then we have that

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$$
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

It is natural to ask what $\mathsf{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$ looks like. This Galois group has four elements, namely

$$\begin{aligned} \sigma_{++}(\sqrt{3} + \sqrt{5}) &= \sqrt{3} + \sqrt{5} \\ \sigma_{+-}(\sqrt{3} + \sqrt{5}) &= \sqrt{3} - \sqrt{5} \\ \sigma_{-+}(\sqrt{3} + \sqrt{5}) &= -\sqrt{3} + \sqrt{5} \\ \sigma_{--}(\sqrt{3} + \sqrt{5}) &= -\sqrt{3} - \sqrt{5} \end{aligned}$$

The decomposition of this group looks like:




In other words, $\mathsf{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}(\sqrt{5})) = \{\sigma_{++},\sigma_{-+}\} \leqslant \{\sigma_{++},\sigma_{+-},\sigma_{-+},\sigma_{--}\} = \mathsf{Gal}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q})$.

**Theorem 5.3.3.** Let $F \subset K \subset E$ be a sequence of extensions, where $K$ is the splitting field of some polynomial $p(x) \in F[x]$. Then for $\sigma \in \mathsf{Gal}(E/F)$, we have $\sigma|_K : K \to K$ is an automorphism from $K$ to $K$ that fixes $F$. Hence $\sigma|_K \in \mathsf{Gal}(K/F)$.

*Proof:* Let $\alpha \in K$, and $q(x) \in F[x]$ a minimal polynomial for $\alpha$. Recall that all $\sigma \in \mathsf{Gal}(E/F)$ will send $\alpha$ to a root of $q(x)$. As all roots of $q(x)$ are in $K$, we have that $\sigma$ takes elements of $K$ to elements of $K$. This proves the result. ■

**Remark 5.3.4.** It is necessary for $K$ to be a splitting field for the above theorem to hold. For example, let $\sigma \in \mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ that takes $\sqrt[3]{2}$ to $\sqrt[3]{2}\omega$. But if $K = \mathbb{Q}(\sqrt[3]{2})$, we have that $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2},\omega) \not\subset \mathbb{Q}(\sqrt[3]{2})$.

**Definition 5.3.5.** Let $G$ be a group. Then $H \leqslant G$ is termed a normal subgroup iff for all $g \in G$ and $h \in H$, $ghg^{-1} \in H$. This relationship is denoted $H \lhd G$.

Note that all subgroups of abelian groups are normal.

**Remark 5.3.6.** Normal subgroups play the same role in group theory as ideals in ring theory.

**Example 5.3.7.** Consider the ring $\mathbb{Z}$ over addition, and its subgroup $2\mathbb{Z}$. Then $\mathbb{Z}/2\mathbb{Z} = \{\{\text{odd numbers}\},\{\text{even numbers}\}\} \approx \mathbb{Z}_2$.

**Theorem 5.3.8.** Let $F \subset K \subset E$ be a sequence of extensions with $K$ a splitting field. Then
1. $\mathsf{Gal}(E/K) \lhd \mathsf{Gal}(E/F)$
2. $\mathsf{Gal}(K/F) \approx \mathsf{Gal}(E/F)/\mathsf{Gal}(E/K)$

*Proof:* **1.** From a previous result, we have that $\mathsf{Gal}(E/K) \leqslant \mathsf{Gal}(E/F)$. Let $\theta \in \mathsf{Gal}(E/K)$ and $\sigma \in \mathsf{Gal}(E/F)$, and $\alpha \in K$. Consider $\sigma^{-1} \circ \theta \circ \sigma \in \mathsf{Gal}(E/F)$, and note that $\sigma(\alpha) \in K$, as $\alpha$ goes to a root of its minimal polynomial. Hence

$$\sigma^{-1}(\theta(\underbrace{\sigma(\alpha)}_{\in K})) = \sigma^{-1}(\sigma(\alpha)) = \alpha$$

Therefore $\sigma^{-1} \circ \theta \circ \sigma \in \mathsf{Gal}(E/K)$, and hence $\mathsf{Gal}(E/K) \lhd \mathsf{Gal}(E/F)$.

**2.** Take $\Psi : \mathsf{Gal}(E/F) \to \mathsf{Gal}(K/F)$ by $\sigma \in \mathsf{Gal}(E/F)$ with $\Psi(\sigma) = \sigma_K$, i.e. $\sigma$ only acting on $K$. As $K$ is a splitting field, if $\alpha \in K$, then $\sigma_K(\alpha) \in K$, so the map is well-defined, and clearly a homeomorphism. Recall that

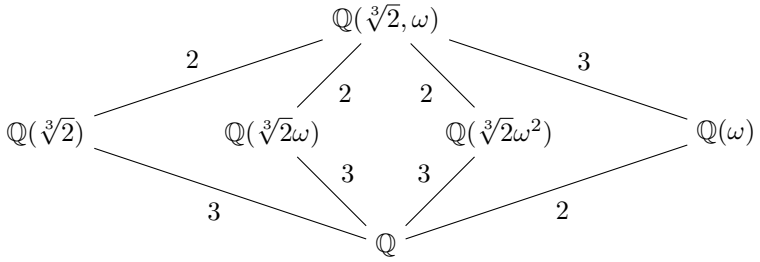
$$\ker(\Psi) = \{\sigma \in \mathsf{Gal}(E/F) \mid \Psi(\sigma) = \mathsf{Id}_{\mathsf{Gal}(K/F)}\}$$

So $\sigma \in \mathsf{Gal}(E/K)$, hence $\ker(\Psi) \subset \mathsf{Gal}(E/K)$. Every $\sigma \in \mathsf{Gal}(K/F)$ may be extended to a $\sigma \in \mathsf{Gal}(E/F)$. Therefore $\Psi(\mathsf{Gal}(E/F)) = \mathsf{Gal}(K/F)$. As for any $\sigma \in \mathsf{Gal}(E/K)$, it follows that $\sigma \in \ker(\Psi)$, and

$$\Psi(\mathsf{Gal}(E/F)) \approx \mathsf{Gal}(E/F)/\ker(\Psi) \implies \mathsf{Gal}(K/F) \approx \mathsf{Gal}(E/F)/\mathsf{Gal}(E/K)$$

■

**Example 5.3.9.** Consider again $\mathbb{Q}(\sqrt[3]{2}, \omega)$. We have that $\mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \approx S_3$. The decomposition is given by:

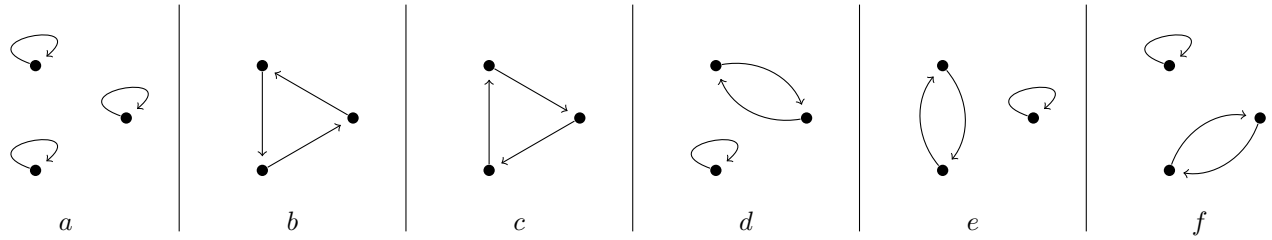



The extension degrees are as given. Further, $\mathbb{Q}(\omega)$ is the splitting field of $x^3 + x + 1$. We can make the folowing relations:

$$\begin{aligned} \mathsf{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) &\approx \mathbb{Z}_2 \\ \mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}(\omega)) &\approx A_3 \approx Z_3 \\ \mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}(\omega)) &\lhd S_3 \end{aligned}$$

**Definition 5.3.10.** Let $H \leqslant \mathsf{Gal}(E/F)$. The field $H' = E^H = \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \ \sigma \in H\}$ is termed the fixed field of $H$.

**Remark 5.3.11.** Let $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, the splitting field of $x^3 - 2$, and $F = \mathbb{Q}$. Then $\mathsf{Gal}(E/F) \approx S_3$. The actions of $\mathsf{Gal}(E/F)$ may be represented by the following diagrams, viewed as superimposed on the complex plane, with the origin at the center, and points a distance $\sqrt[3]{2}$ away from the origin:




Then the subgroups of $\mathsf{Gal}(E/F)$ and their respective fixed fields are given by:

$$\begin{aligned} \{a\} &\to \mathbb{Q}(\sqrt[3]{2}, \omega) \\ \{a, d\} &\to \mathbb{Q}(\sqrt[3]{2}\omega^2) \\ \{a, e\} &\to \mathbb{Q}(\sqrt[3]{2}) \\ \{a, f\} &\to \mathbb{Q}(\sqrt[3]{2}\omega) \\ \{a, b, c\} &\to \mathbb{Q}(\omega) \\ \{a, b, c, d, e, f\} &\to \mathbb{Q} \end{aligned}$$

Note that the extensions of $\mathbb{Q}$ are given by what element each group fixes.

**Theorem 5.3.12.** Let $E$ be an extension field of $F$, with $[E : F] = n$. Then the following are equivalent:

1. $E^{\mathsf{Gal}(E/F)} = F$
2. If $p(x) \in F[x]$ is irreducible with a root $\alpha \in E$, then $p(x)$ splits and is separable in $E$
3. $E$ is the splitting field of a separable polynomial

*Proof:* (**1.** $\Rightarrow$ **2.**) Let $E^{\mathsf{Gal}(E/F)} = F$. Assume that $E \neq F$, so let $p(x) \in F[x]$ be irreducible in $F[x]$ with a root $\alpha \in E$. Let $\alpha_1, \ldots, \alpha_n$ be all the possible images of $\alpha$ under $\sigma \in \mathsf{Gal}(E/F)$. Let $h(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, and as $\sigma$ is a permutation of the set $\{\alpha_1, \ldots, \alpha_n\}$, it follows that

$$\sigma(h(x)) = \underbrace{(x-\alpha_1)\cdots(x-\alpha_n)}_{\text{possibly in different order}} = h(x)$$

So for $h(x) = \sum_{i=0}^{n} a_i x^i$, the $a_i$ are fixed by $\sigma$ for all $\sigma \in \mathsf{Gal}(E/F)$ (equivalently $E^{\mathsf{Gal}(E/F)} = F$), so $h(x) \in F[x]$. Since $h$ splits and is separable in $E$, and as $p(x) \mid h(x)$, it follows that $p(x)$ splits and is separable in $E$.

(**2.** $\Rightarrow$ **3.**) Assume that if $p(x)$ is irreducible with a root $\alpha_1 \in E$, then $p(x)$ splits and is separable. Let $E$ be a finite extension of $F$, and $\alpha_1 \in E \setminus F$ (if $E = F$, then the proof is trivial). For $p_1(x)$ the minimal polynomial of $\alpha_1$, let $E_1$ be the splitting field of $p_1(x)$, for which $F \subset E_1 \subset E$. Now take $\alpha_2 \in E \setminus E_1$, and let $p_2(x)$ be the minimal polynomial of $\alpha_2$ over $F$. Then $p_2(x)$ splits over $E_1$, and $\gcd(p_1(x), p_2(x)) = 1$. For $E_2$ the splitting field of $p_1(x)p_2(x)$, it follows that $F \subset E_1 \subset E_2 \subset E$.

Repeat this process finitely many times, guaranteed to be finite, as $E$ is a finite extension of $F$. Then we will have $E = E_n$ for some $n \in \mathbb{N}$, the splitting field of some polynomial $p_1(x)p_2(x)\cdots p_n(x)$.

(**3.** $\Rightarrow$ **1.**) Assume that $E$ is the splitting field of a separable polynomial. Note that $F \subset E^{\mathsf{Gal}(E/F)} \subset E$, hence $\mathsf{Gal}(E/E^{\mathsf{Gal}(E/F)}) \leqslant \mathsf{Gal}(E/F)$. Note that if $\sigma \in \mathsf{Gal}(E/F)$, then $\sigma$ will fix $E^{\mathsf{Gal}(E/F)}$ by definition, hence $\mathsf{Gal}(E/E^{\mathsf{Gal}(E/F)}) = \mathsf{Gal}(E/F)$. Further,

$$|\mathsf{Gal}(E/F)| = [E:F] = \left[E : E^{\mathsf{Gal}(E/F)}\right]\left[E^{\mathsf{Gal}(E/F)} : F\right] = \left|\,\mathsf{Gal}\left(E/E^{\mathsf{Gal}(E/F)}\right)\right|\left[E^{\mathsf{Gal}(E/F)} : F\right]$$

Since $\mathsf{Gal}(E/F) = \mathsf{Gal}(E/E^{\mathsf{Gal}(E/F)})$, it follows that $[E^{\mathsf{Gal}(E/F)} : F] = 1$. Hence $E^{\mathsf{Gal}(E/F)} = F$. ■

**Definition 5.3.13.** If $E$ satisfies the statements above, then $E$ is termed a Galois extension of $F$.

**Example 5.3.14.** The field $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $x^3 - 2$, which is a separable polynomial, so $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})} = \mathbb{Q}$.

**Theorem 5.3.15.** [Fundamental theorem of Galois theory]
Let $E$ be a Galois extension of $F$, and let $\chi$ be a map from the set of subfields of $E$ to the set of subgroups of $\mathsf{Gal}(E/F)$, such that $\chi(K) = \mathsf{Gal}(E/K) \leqslant \mathsf{Gal}(E/F)$. Then:

1. $\chi$ is injective
2. $K = E^{\mathsf{Gal}(E/K)} = E^{\chi(K)}$
3. $\chi(E^H) = H$ for $H \leqslant G = \mathsf{Gal}(E/F)$
4. $[E:K] = |\mathsf{Gal}(E/K)| = |\chi(K)|$
5. $[K:F] = |\mathsf{Gal}(E/F)|/|\mathsf{Gal}(E/K)|$
6. $K$ is a galois extension of $F$ iff $\mathsf{Gal}(E/K) = \chi(K) \lhd \mathsf{Gal}(E/F)$
7. $K_1 \subset K_2$ iff $\chi(K_2) \leqslant \chi(K_1)$

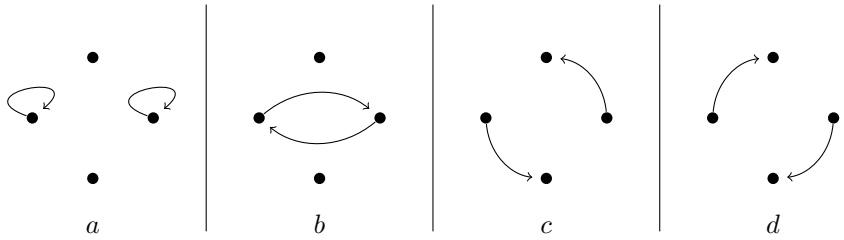
Before we prove this, we look to an application of the theorem. The restatement and proof will follow afterward.

**Example 5.3.16.** Let $E$ be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Find all subfields of $E$ and all subgroups of $\mathsf{Gal}(E/\mathbb{Q})$, exhibiting the correspondence.

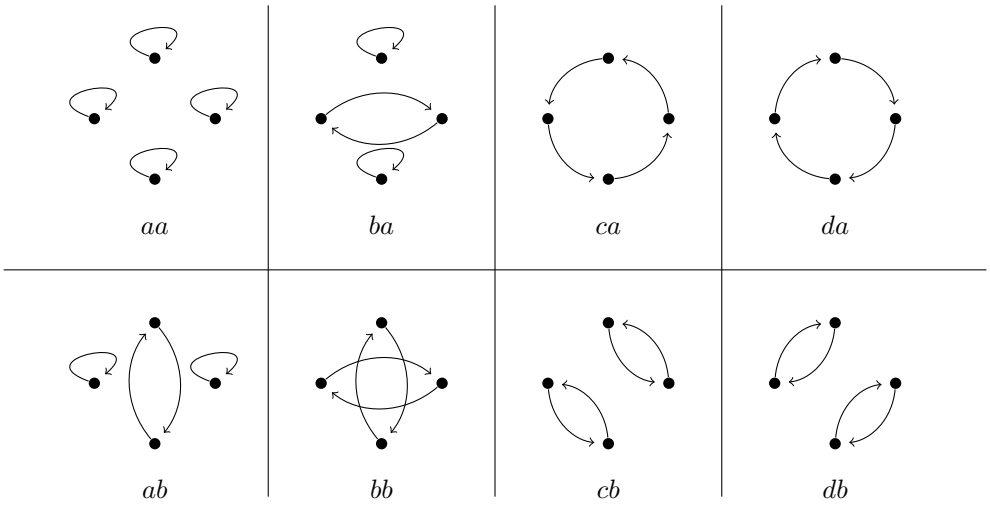
First, the splitting field is

$$\begin{aligned} E &= \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i) \\ &= \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i) \\ &= \mathbb{Q}(\sqrt[4]{2}, i) \end{aligned}$$

Note that if $\sigma \in \mathsf{Gal}(E/\mathbb{Q})$, then $\sigma(\sqrt[4]{2}) = \pm\sqrt[4]{2}$ or $\pm\sqrt[4]{2}i$. Hence there are four distinct actions, given by:



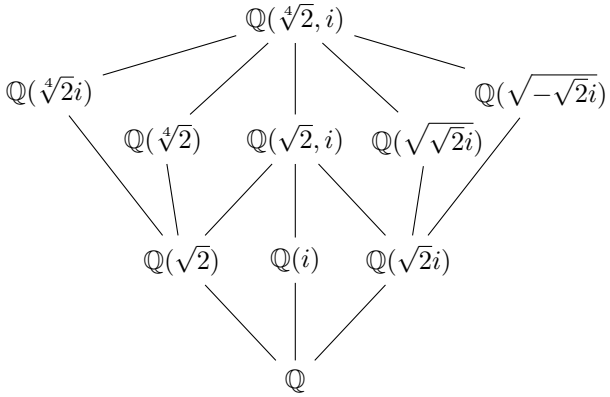

Above we have only considered the possible destinations of $\pm\sqrt[4]{2}$, and we stil have to account for $\pm\sqrt[4]{2}i$. For each of the maps above, this gives two new maps.

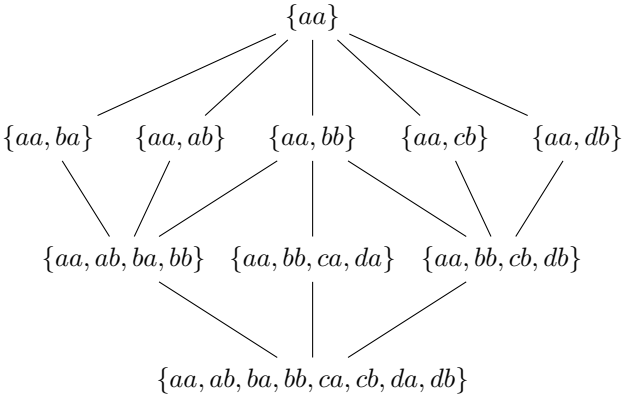



Hence $\mathsf{Gal}(E/F)$ is a group with 8 elements. Its subgroups and corresponding subgroups are:

$$\begin{array}{rcl@{\qquad}rcl}
\{aa\} & \to & \mathbb{Q}(\sqrt[4]{2}, i) & \{aa, db\} & \to & \mathbb{Q}(\sqrt{-\sqrt{2}i}) \\
\{aa, ba\} & \to & \mathbb{Q}(\sqrt[4]{2}i) & \{aa, bb, ca, da\} & \to & \mathbb{Q}(i) \\
\{aa, ab\} & \to & \mathbb{Q}(\sqrt[4]{2}) & \{aa, ab, ba, bb\} & \to & \mathbb{Q}(\sqrt{2}) \\
\{aa, bb\} & \to & \mathbb{Q}(\sqrt{2}, i) & \{aa, bb, cb, db\} & \to & \mathbb{Q}(\sqrt{2}i) \\
\{aa, cb\} & \to & \mathbb{Q}(\sqrt{\sqrt{2}i}) & \{aa, ab, ba, bb, ca, cb, da, da\} & \to & \mathbb{Q}
\end{array}$$

This may be represented diagrammatically as:



All the extensions have degree 2.

**Theorem 5.3.15.** [Fundamental theorem of Galois theory]
Let $E$ be a Galois extension of $F$, and let $\chi$ be a map from the set of subfields of $E$ to the set of subgroups of $\mathsf{Gal}(E/F)$, such that $\chi(K) = \mathsf{Gal}(E/K) \leqslant \mathsf{Gal}(E/F)$. Then:

1. $\chi$ is injective
2. $K = E^{\mathsf{Gal}(E/K)} = E^{\chi(K)}$
3. $\chi(E^H) = H$ for $H \leqslant G = \mathsf{Gal}(E/F)$
4. $[E : K] = |\mathsf{Gal}(E/K)| = |\chi(K)|$
5. $[K : F] = |\mathsf{Gal}(E/F)|/|\mathsf{Gal}(E/K)|$
6. $K$ is a galois extension of $F$ iff $\mathsf{Gal}(E/K) = \chi(K) \lhd \mathsf{Gal}(E/F)$
7. $K_1 \subset K_2$ iff $\chi(K_2) \leqslant \chi(K_1)$

*Proof:* **1.** Implied by **2.** and **3.**

**2.** So $E$ is a Galois extension of $F$, i.e. the splitting field of a separable polynomial $p(x)$ over $F$. Hence $E$ is a Galois extension over $K$, as it is the splitting field of $p(x)$. And by the definition of a Galois extension, $K = E^{\mathsf{Gal}(E/K)}$.

**3.** We wish to show that $\mathsf{Gal}(E/E^H) = H$. First notice that if $\sigma \in H$, then for all $\alpha \in E^H$, we have $\sigma(\alpha) = \alpha$, hence $H \leqslant \mathsf{Gal}(E/E^H)$. Describe $H$ by

$$H = \{\sigma_1, \ldots, \sigma_\ell\} \qquad \text{where} \qquad |\mathsf{Gal}(E/E^H)| = n \geqslant \ell$$

As $E$ is Galois, it is the splitting field of a separable polynomial, so it is simple. Hence there exists $\alpha \in E$ such that $E = E^H(\alpha)$, with the degree of the minimal polynomial in $E^H[x]$ of $\alpha$ being $n$. Define the polynomial $p(x)$ by

$$p(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_\ell(\alpha)) = \sum_{i=0}^{\ell} a_i x^i$$

Then $p(x) \in E^H[x]$, and as $\ell \leqslant n$ and the minimal polynomial of $\alpha$ of degree $n$ divides $p(x)$, it follows that $\ell = n$. Hence $H = \mathsf{Gal}(E/E^H)$.

**4.** This has been proven earlier, in (5.3.12).

**5.** Consider the following identities:

$$\begin{aligned} [E : K] &= |\mathsf{Gal}(E/K)| \\ [E : F] &= |\mathsf{Gal}(E/F)| \\ [E : F] &= [E : K][K : F] \end{aligned}$$

Solving for $[K : F]$ gives the result.

**6.** It has already been shown that if $K$ is Galois, then $\mathsf{Gal}(E/K) \lhd \mathsf{Gal}(E/F)$, hence we start with the assumption that $\mathsf{Gal}(E/K) \lhd \mathsf{Gal}(E/F)$. As $E$ is Galois over $F$, $E$ is Galois over $K$. Let $p(x)$ be an irreducible polynomial in $F[x]$ with a root $\alpha \in K$. The field $K$ being Galois is equivalent to $p(x)$ splitting and being separable, and as $p(x)$ splits and is separable in $E$, it remains to show that all roots of $p(x)$ are in $K$.

Let $\sigma \in \mathsf{Gal}(E/F)$ with $\sigma(\alpha) = \beta$, another root of $p(x)$. For $\theta \in \mathsf{Gal}(E/K)$, we have that $\sigma^{-1} \circ \theta \circ \sigma \in \mathsf{Gal}(E/K)$, as $\mathsf{Gal}(E/K)$ is normal, meaning that $(\sigma^{-1} \circ \theta \circ \sigma)(\alpha) = \alpha$. Hence

$$(\theta \circ \sigma)(\alpha) = \sigma(\alpha) \implies \theta(\beta) = \beta$$

Hence $\beta$ is fixed by $\mathsf{Gal}(E/K)$, and $\beta \in E^{\mathsf{Gal}(E/K)} = K$. So all roots of $p(x)$ are in $K$, hence $p(x)$ splits over $K$, so $K$ is Galois over $F$.

**7.** Given the sequence of extensions $F \subset K_1 \subset K_2 \subset E$, it follows that $\mathsf{Gal}(E/K_2) \leqslant \mathsf{Gal}(E/K_1) \leqslant \mathsf{Gal}(E/K)$. ■

# Index



# Mathematicians