Algebra Summary

Ánoq of the Sun, Hardcore Processing *

June 30, 2004

1 The Numbers

General

- ***Composition*** $\stackrel{def}{=}$ ⟨(1.2) p. 2 ∈ [1]⟩
  a *map* from a *pair* of *numbers* to a *new number*: $\mathbb{L} \times \mathbb{L} \to \mathbb{L}$

Misc

- Basic fact about the real numbers $\mathbb{R}$:
  Any *non-empty set* of real numbers which is *upwards limited*
  has a *supremum.* ⟨p. 2 ∈ [1]⟩

Identities

$x + y = y + x$	(commutativity)	a0	⟨p. 1 ∈ [1]⟩
$x + (y + z) = (x + y) + z$	(associativity)	a1	⟨p. 1 ∈ [1]⟩
$x + 0 = 0 + x = x$	(neutral element)	a2	⟨p. 1 ∈ [1]⟩
$x + (-x) = (-x) + x = 0$	(inverse element)	a3	⟨p. 1 ∈ [1]⟩
$xy = yx$	(commutativity)	m0	⟨p. 1 ∈ [1]⟩
$x(yz) = (xy)z$	(associativity)	m1	⟨p. 1 ∈ [1]⟩
$x1 = 1x = x$	(neutral element)	m2	⟨p. 1 ∈ [1]⟩
$xx^{-1} = x^{-1}x = 1$, for $x \neq 0$	(inverse element)	m3	⟨p. 1 ∈ [1]⟩
$x = y$ eller $x < y$ eller $y < x$	(comparability / totality)	o0	⟨p. 1 ∈ [1]⟩
$x \not< x$	(irreflexivity)	o1	⟨p. 1 ∈ [1]⟩
$x < y \wedge y < z \Rightarrow x < z$	(transitivity)	o2	⟨p. 1 ∈ [1]⟩
$x(y + z) = xy + xz$, $(x + y)z = xz + yz$	(distributivity)	am	⟨p. 1 ∈ [1]⟩
$x < y \Rightarrow x + z < y + z$	(harmony)	ao	⟨p. 1 ∈ [1]⟩
$x < y \wedge 0 < z \Rightarrow xz < yz$	(harmony)	mo	⟨p. 1 ∈ [1]⟩

About Addition Identities $a0 - a3$

- Identities $a0 - a3$ is about *addition*,
  which is a *composition* of numbers: $(x, y) \mapsto x + y$. ⟨(1.2) p. 2 ∈ [1]⟩

- *Addition* of *real numbers* with $a0 - a3$ constitutes a *commutative group.*
  ⟨p. 2 ∈ [1]⟩

- Associativity says: ⟨(1.2) p. 2 ∈ [1]⟩
  Finite sums do not need a specific *order of computation of addition.*

- Commutativity says: ⟨(1.2) p. 2 ∈ [1]⟩
  Left and *right elements* behave the same.

- About *neutral element*: It is *unique.* ⟨(1.2) p. 2 ∈ [1]⟩

- About *inverse element*: ⟨(1.2.1) p. 2 ∈ [1]⟩
  - **The *difference* between 2 numbers** $x - y \overset{def}{=} x + (-y)$
  - *Adding* and then *adding the inverse* does *not alter* a number: $(y + x) + (-x) = y$

About Multiplication Identities $a0 - a3$

- Identities $m0 - m3$ is about *multiplication*,
  which is a *composition* of numbers *except* 0: $(x, y) \mapsto x \cdot y$. ⟨(1.3) p. 3 ∈ [1]⟩

- The *numbers excluding* 0 with the *multiplication rules* $m0 - m3$ constitutes a *commutative group.* ⟨(1.3) p. 3 ∈ [1]⟩

- The *inverse element* x^{-1} is called the ***reciprocal*** of x (only for $x \neq 0$). ⟨(1.3) p.3 ∈ [1]⟩

- **The *quotient* of 2 numbers** $y/x \overset{def}{=} yx^{-1}$ ⟨(1.3) p.3 ∈ [1]⟩

- The *zero rule* imply: $x \neq 0 \wedge y \neq 0 \Rightarrow x \cdot y \neq 0$. ⟨(1.3) p.3 ∈ [1]⟩

About Ordering Identities $o0 - o2$

- Identities $o0 - o2$ is about *ordering*,
  which is a *relation* between numbers: $x < y \equiv y > x$. ⟨(1.4) p. 3 ∈ [1]⟩

- **The *positive* numbers** $\overset{def}{=} \{x \mid x > 0\}$ ⟨(1.4) p. 3 ∈ [1]⟩

- **The *negative* numbers** $\overset{def}{=} \{x \mid x < 0\}$ ⟨(1.4) p. 3 ∈ [1]⟩

- About *totality* ($o0$): Any x is *comparable.*
  Any $x \neq 0$ is thus either *positive* or *negative.* ⟨(1.4) p. 3 ∈ [1]⟩

- About *irreflexibility* ($o1$): $x < y$ is the *sharp inequality.* ⟨(1.4) p. 3 ∈ [1]⟩

- ***Less than or equal*** $\leq \overset{def}{=} x \leq y \Leftrightarrow x < y \vee x = y$. ⟨(1.4) p. 3 ∈ [1]⟩

- ***Reflexibility*** $\overset{def}{=} x \leq x$.
  Holds for $\leq$ and is the *opposite* of *irreflexibility.* ⟨(1.4) p. 4 ∈ [1]⟩

- *Transitivity* ($o2$) also holds for $\leq$. ⟨(1.4) p. 3 ∈ [1]⟩

About Harmonical Identities am, ao **and** mo

- *Distributivity* (am): *Multiplication* is *distributive* w.r.t. *addition.*
  The harmonious relationship between *addition* and *multiplication.*
  ⟨(1.5) p. 3 ∈ [1]⟩
  - It extends to: $x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n$. ⟨(1.5.1) p. 3 ∈ [1]⟩
  - More generally: $(x_1 + \cdots + x_n)(y_1 + \cdots + y_n) = \sum x_i y_j$.
    "A *product of sums* equals the *sum of all products* which as it's *factors* have an element from each of the sums".
  - Even more generally (also with more than 24 sums :-) ⟨(1.5.2) p. 3 ∈ [1]⟩
    $(\sum a_\alpha)(\sum b_\beta)\cdots(\sum x_\omega) = \sum a_\alpha b_\beta \cdots x_\omega$
- From the *distributive law* (and *addition rules*) follow:
  $0 \cdot y = 0$
  $(-x)y = -(xy)$
  $(-1)y = -y$
- *Binomial formula*: ⟨ex. 1.6 p. 4 ∈ [1]⟩
  $\forall n \in \mathbb{N} : (x + y)^n = \sum_{i=1}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) x^i y^{n-1}$.
- *Harmony*: Expresses the harmony between *addition* and *order* (ao) and *multiplication* and *order* (mo). ⟨(1.7) p. 4 ∈ [1]⟩
  - It follows that x *positive* $\Leftrightarrow -x$ *negative.* ⟨(1.7) p. 4 ∈ [1]⟩
  - and: $x < y \Leftrightarrow 0 < y - x$
  - *Multiplication* by *negative* numbers *flips inequalities*:
    $x < y \wedge z < 0 \Rightarrow zx > zy$ ⟨(1.7) p. 4 ∈ [1]⟩
  - *Multiplication by*: ⟨p. 4 ∈ [1]⟩
    $$\begin{array}{lcl} x, y > 0 & \Rightarrow & x \cdot y > 0 \\ x, y < 0 & \Rightarrow & x \cdot y > 0 \\ x < 0 \wedge y > 0 \text{ (or vice versa)} & \Rightarrow & x \cdot y < 0 \end{array}$$
- The *zero rule*:
  $xy = 0 \quad \Leftrightarrow x = 0 \vee y = 0$ ⟨(1.8.1) p. 5 ∈ [1]⟩
  $xy \neq 0 \quad \Leftrightarrow x \neq 0 \wedge y \neq 0$ ⟨(1.8.2) p. 5 ∈ [1]⟩
- **The *numerical value*** $|x|$ **of** $x \overset{def}{=}$
  the *biggest* of x and $-x$. ⟨(1.9) p. 5 ∈ [1]⟩
- The following holds about $|\cdot|$: ⟨(1.9) p. 5 ∈ [1]⟩
  $$\begin{array}{ll} |-x| = |x| & \text{(n1)} \\ |x| \geq 0 & \text{(n2a)} \\ |x| = 0 \Rightarrow x = 0 & \text{(n2b)} \\ |x + y| \leq |x| + |y| & \text{(n3)} \\ |xy| = |x||y| & \text{(n4)} \end{array}$$

1.1 The Natural Numbers

- For the *natural numbers* $\mathbb{N} = \{1, 2, 3, \dots\}$ the *usual rules* for numbers apply *except* rules about 0, *inverse element* and *reciprocal element*, i.e.: ⟨p. 7 ∈ [1]⟩

$x + y = y + x$	(commutativity)	a0
$x + (y + z) = (x + y) + z$	(associativity)	a1
$xy = yx$	(commutativity)	m0
$x(yz) = (xy)z$	(associativity)	m1
$x1 = 1x = x$	(neutral element)	m2
$x = y$ eller $x < y$ eller $y < x$	(comparability / totality)	o0
$x \nless x$	(irreflexivity)	o1
$x < y \wedge y < z \Rightarrow x < z$	(transitivity)	o2
$x(y + z) = xy + xz$, $(x + y)z = xz + yz$	(distributivity)	am
$x < y \Rightarrow x + z < y + z$	(harmony)	ao
$x < y \Rightarrow xz < yz$ (since $\forall z \in \mathbb{N} : z > 0$)	(harmony)	mo
$x < x + 1$	does *not* follow from only the above rules	

- $d \in \mathbb{N}$ **is *divisor* in** $n \in \mathbb{N}$ a.k.a. $d|p \overset{def}{=} \exists c \in \mathbb{N} : c \cdot d = n$.

- $p \in \mathbb{N}$ **is a *prime number*** $\overset{def}{=}$
  $p > 1$ and *only* 1 and p are *divisors* in p. ⟨ex. (2.3) p. 8 ∈ [1]⟩

- $p \in \mathbb{N}$ **is a *composite number*** $\overset{def}{=}$
  $p = kd$ where $k, d > 1$. ⟨ex. (2.3) p. 8 ∈ [1]⟩

- $p \in \mathbb{N}$ **is a *prime divisor* of** $n \in \mathbb{N}$ $\overset{def}{=}$
  p is *prime* and *divisor* in n. ⟨ex. (2.3) p. 8 ∈ [1]⟩

- $\forall n \in \mathbb{N} : n$ has a *prime divisor*. ⟨ex. (2.3) p. 8 ∈ [1]⟩

- If p is the *smallest divisor* in $n \in \mathbb{N}$, then p is *prime*. ⟨ex. (2.3) p. 8 ∈ [1]⟩

- $n \in \mathbb{N}$ **has a *prime resolution*** $\overset{def}{=}$ ⟨ex. (2.9) p. 9 ∈ [1]⟩
  There *exists primes* $p_1, p_2, \dots, p_s$ such that: $n = p_1 \cdot p_2 \cdot \dots \cdot p_s$.

- $\forall n \in \mathbb{N} : n$ has a *prime resolution*. ⟨ex. (2.9) p. 9 ∈ [1]⟩

- $\forall n \in \mathbb{N} : 1^2 + 2^2 + \dots + n^2 = n(n + 1)(2n + 1)/6$. ⟨ex. (2.6) p. 8 ∈ [1]⟩

1.2 The Integers

- For the *integers* $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ the *usual rules* for numbers apply *except* rules about *reciprocal element*, i.e.: ⟨p. 13 ∈ [1]⟩

$x + y = y + x$	(commutativity)	a0
$x + (y + z) = (x + y) + z$	(associativity)	a1
$x + 0 = 0 + x = x$	(neutral element)	a2
$x + (-x) = (-x) + x = 0$	(inverse element)	a3
$xy = yx$	(commutativity)	m0
$x(yz) = (xy)z$	(associativity)	m1
$x1 = 1x = x$	(neutral element)	m2
$\forall x, y \in \mathbb{Z} : x = y \vee x < y \vee y < x$	(comparability / totality)	o0
$\forall x \in \mathbb{Z} : x \nleq x$	(irreflexivity)	o1
$x < y \wedge y < z \Rightarrow x < z$	(transitivity)	o2
$x(y + z) = xy + xz$, $(x + y)z = xz + yz$	(distributivity)	am
$x < y \Rightarrow x + z < y + z$	(harmony)	ao
$x < y \wedge 0 < z \Rightarrow xz < yz$	(harmony)	mo

- $d \in \mathbb{Z}$ **is *divisor* in** $a \in \mathbb{Z}$ a.k.a. a **is *a multiple* of** d a.k.a. $d|a \overset{def}{=}$ $\exists q \in \mathbb{Z} : a = q \cdot d$. ⟨(3.2) p. 13 ∈ [1]⟩

- $d \in \mathbb{Z}$ is a *divisor* in $a \in \mathbb{Z} \Leftrightarrow (-d)|a$. ⟨(3.2) p. 13 ∈ [1]⟩

- For *any divisor* $d \in \mathbb{Z}$ in $a \in \mathbb{Z}$, $a \neq 0$ we have $|d| \leq |a|$ ⟨(3.2.1) p. 13 ∈ [1]⟩

- **The *trivial divisors* of** $a \in \mathbb{Z} \overset{def}{=}$ ± 1 and $\pm a$ (which are *always divisors* of a) ⟨p. 13 ∈ [1]⟩

- $p \in \mathbb{Z}$ **is a *prime number*** $\overset{def}{=}$ $p > 1$ and *has only trivial divisors.* ⟨p. 13 ∈ [1]⟩

- **A *common divisor*** a.k.a. ***common denominator* of** $a, b \in \mathbb{Z} \overset{def}{=}$ $q \in \mathbb{Z}$ such that $(q|a) \wedge (q|b)$. ⟨(3.2) p. 13 ∈ [1]⟩

- $\mathbf{gcd}(a, b) \overset{def}{=}$ the *greatest common divisor* of $a, b \in \mathbb{Z}$. ([1] uses the notation: $d = (a, b)$). ⟨p. 14 ∈ [1]⟩

- $a, b \in \mathbb{Z}$ **are *(mutually) primic*** $\overset{def}{=} gcd(a, b) = 1$. ⟨(3.2) p. 14 ∈ [1]⟩

- $\mathbf{gcd}(a_1, \dots, a_r)$ where $a_1, \dots, a_r \in \mathbb{Z}$ and *at least one* $a_i \neq 0 \overset{def}{=}$ the *greatest divisor*, i.e. $q \in \mathbb{Z}$ such that $(q|a_1), \dots, (q|a_r)$. ([1] uses the notation: $d = (a_1, \dots, a_r)$). ⟨(3.2) p. 14 ∈ [1]⟩

- $a_1, \dots, a_r \in \mathbb{Z}$ **are *(mutually) primic*** $\overset{def}{=}$ $\forall i \neq j : gcd(a_i, a_j) = 1$. ⟨(3.2) p. 14 ∈ [1]⟩

- **The *least common multiple* of** $a_1, \dots, a_r \in \mathbb{Z} \overset{def}{=}$ the *smallest* $m \in \mathbb{Z}$ such that $(a_1|m), \dots, (a_r|m)$. ⟨(3.2) p. 14 ∈ [1]⟩

- For *prime number* $p \in \mathbb{N}$: ⟨(3.2) p. 14 ∈ [1]⟩ p is *mutually primic* with $a \in \mathbb{Z} \Leftrightarrow p$ is *not divisor* in a.

Misc Useful Theorems

- $\forall n, k \in \mathbb{N} : gcd(n, n+k) \leq k$.
- $\forall a, b \in \mathbb{N} : ab = dm$, where ⟨exc. 6 p. 20 ∈ [1]⟩
  $d = gcd(a, b)$ and m is the *least common multiple* of a and b.

Division and Remainder

- *Division Theorem*: For a *given* $d \in \mathbb{N}$ then: ⟨(3.4) p. 147 ∈ [1]⟩
  $\forall a \in \mathbb{Z} : \exists q, r \in \mathbb{Z} : (a = qd + r)$ and $(0 \leq r < d)$.
- For a *given* $d \in \mathbb{N}$:
  A *remainder* r of $a \in \mathbb{Z}$ *under division* by d $\stackrel{def}{=}$
  $r = a - qd$ for some q. ⟨(3.5) p. 147 ∈ [1]⟩
- For a *given* $d \in \mathbb{N}$:
  The *principal remainder* of $a \in \mathbb{Z}$ *divided* by d $\stackrel{def}{=}$
  The *unique remainder* r (as in the *division theorem*) given by $0 \leq r < d$.
  I.e.: The *smallest non-negative remainder.* ⟨(3.5) p. 147 ∈ [1]⟩
- For a *given* $d \in \mathbb{N}$:
  The *numerically smallest remainder* of $a \in \mathbb{Z}$ *divided* by d $\stackrel{def}{=}$
  The *unique remainder* s determined by $a = qd + s$ and $-\frac{d}{2} < s \leq \frac{d}{2}$.
  If r is the *principal remainder* then: ⟨(3.5) p. 147 ∈ [1]⟩
  a) $(r \leq \frac{d}{2}) \quad \Rightarrow \quad s = r$
  b) $(r > \frac{d}{2}) \quad \Rightarrow \quad s = r - d$

Common Divisors and Theorems About Primicness

- *Euklid's algorthm* for finding the *greatest common denominator*:
  Define the function *gcd* by (using Standard ML-like notation):
  fun $gcd(r_i, r_j) =$ if $r_j > 0$ then $gcd(r_j, r_i \; mod \; r_j)$ else r_i.
  Then: $gcd(a, b)$ returns the *greatest common denominator* of a and b assuming $a \geq b > 0$. ⟨(3.6) p. 15, ex. (3.8) p. 16 ∈ [1]⟩

- For $a, b \in \mathbb{Z}$ where at least either a or $b \neq 0$:
  The *common divisors* in a and b are *exactly* the *divisors* in $gcd(a, b)$.
  Furthermore: There *exists* $x, y \in \mathbb{Z}$ such that:
  $gcd(a, b) = xa + yb$ (calculate backwards in *Euklid's algorithm*).
  ⟨thm. (3.7) p. 15 ∈ [1]⟩

- $a, b \in \mathbb{Z}$ are *primic* $\Leftrightarrow \exists x, y \in \mathbb{Z} : 1 = xa + yb$. ⟨cor. (3.9) p. 16 ∈ [1]⟩

- If a *primic* with b_1 and with b_2, then
  a *primic* with the *product* $b_1 b_2$. ⟨cor. (3.10) p. 16 ∈ [1]⟩

Divisor and Prime Theorems

- Let $a, b, n \in \mathbb{Z}, n \neq 0$ and $d = gcd(a, n)$. Then: $n|ab \Leftrightarrow \frac{n}{d}|b$.
  In particular, for a and n *primic* (i.e. $gcd(a, n) = 1$): $n|ab \Leftrightarrow n|b$.
  ⟨cor. (3.11) p. 16 ∈ [1]⟩

- Let $n = n_1 \cdot \dots \cdot n_r$ be a product of *pairwise primic natural numbers* n_i.
  Then: $\forall a \in \mathbb{Z} : (n|a \Leftrightarrow \forall n_i : n_i|a)$. ⟨cor. (3.12) p. 17 ∈ [1]⟩

- For *prime* p and $a, b \in \mathbb{Z}$: $p|ab \Leftrightarrow (p|a \vee p|b)$. ⟨lemma 3.13 p. 17 ∈ [1]⟩

- For *prime* p and $a_1, \dots, a_s \in \mathbb{Z}$: $p|(a_1 \cdot \dots \cdot a_s) \Leftrightarrow \exists i \in \{1, \dots, s\} : p|a_i$.
  ⟨"⇒": obs. 3.14 p. 17, "⇐": trivial ∈ [1]⟩

- Euclid's Theorem: There are *infinitely many primes*. ⟨thm. (3.15) p. 17 ∈ [1]⟩
  Given k *primes* $p_1, \dots, p_k$, then
  $p_1 \cdot \dots \cdot p_k + 1$ is a number with a *new prime divisor*.

- Dirichlet's Theorem: For $gcd(a, b) = 1$ where $a, b \in \mathbb{N}$,
  there *exists infinitely many primes* of the form $ad + b$, where $d \in \mathbb{N}$.

Prime Resolution Theorems

- Any $a \in \mathbb{Z}, a > 1$ has a *unique prime resolution* $a = p_1 \cdot \dots \cdot p_s$.
  Unique means: Given 2 prime resolutions $a = p_1 \cdot \dots \cdot p_s$, $a = q_1 \cdot \dots \cdot q_t$,
  Then $s = t$, and by appropriate renumbering of q_j we have
  $\forall i \in \{1, \dots, s\} : q_i = p_i$.
  $\langle$Fundamental Theorem of Arithmetics, thm. (3.16) p. 18 $\in$ [1]$\rangle$

- *About Prime Resolutions*: $\langle$(3.17) p. 18-19 $\in$ [1]$\rangle$

  - Prime resolutions may contain *duplicates* of *primes*.
    They may be rewritten to the form:
    $p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$ where $p_1, \dots, p_r$ are *distinct* and $\alpha_1, \dots, \alpha_r \geq 1$.
  - Considering prime resolutions of a *finite* set of numbers,
    we may assume the *same primes* p_j for *all* their prime resolutions.
  - We can formally define: $1 = p_1^0 \cdot \dots \cdot p_r^0$.
  - *Uniqueness implies* that for: $p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} = p_1^{\beta_1} \cdot \dots \cdot p_r^{\beta_r}$, where
    $p_1, \dots, p_r$ are *distinct* we have: $\forall i \in \{1, \dots, r\} : \alpha_i = \beta_i$.
  - We can determine the *positive divisors* of $a \in \mathbb{Z}_+$ from the
    prime resolution $a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$.
    Consider $q, d \in \mathbb{Z}_+$ with *prime resolutions*:
    $q = p_1^{\nu_1} \cdot \dots \cdot p_r^{\nu_r}$, $d = p_1^{\delta_1} \cdot \dots \cdot p_r^{\delta_r}$.
    From this we get: $qd = p_1^{\nu_1+\delta_1} \cdot \dots \cdot p_r^{\nu_r+\delta_r}$.
    So $a = qd \Leftrightarrow \forall j \in \{1, \dots, r\} : \alpha_j = \nu_j + \delta_j$.
  - $d = p_1^{\delta_1} \cdot \dots \cdot p_r^{\delta_r}$ is *divisor* in $a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r} \Leftrightarrow$
    $\forall j \in \{1, \dots, r\} : 0 \leq \delta_j \leq \alpha_j$.
    Notice: $d = 1 \Rightarrow \delta_1 = \dots = \delta_r = 0$
    and $d = a \Rightarrow \delta_1 = \alpha_1, \dots, \delta_r = \alpha_r$.
  - The number n of *positive divisors* in $a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$ is the product:
    $n = (\alpha_1 + 1) \cdot \dots \cdot (\alpha_r + 1)$.
  - For $a, b, d \in \mathbb{Z}$ with prime resolutions:
    $a = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}, b = p_1^{\beta_1} \cdot \dots \cdot p_r^{\beta_r}, d = p_1^{\delta_1} \cdot \dots \cdot p_r^{\delta_r}$ then:
    * d is a *common denominator* of a and b if and only if
      $\forall j \in \{1, \dots, r\} : \delta_j \leq \alpha_j \wedge \delta_j \leq \beta_j$, i.e.:
      $\forall j \in \{1, \dots, r\} : \delta_j \leq \min\{\alpha_j, \beta_j\}$.
      $gcd(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} \cdot \dots \cdot p_r^{\min\{\alpha_r,\beta_r\}}$.
    * l is the *least common multiple* of a and b if and only if
      $l = p_1^{\max\{\alpha_1,\beta_1\}} \cdot \dots \cdot p_r^{\max\{\alpha_r,\beta_r\}}$.

- For a *prime power* $a = p^\alpha$ the *positive divisors* in a are *exactly*:
  $\{p^\delta \mid 0 \leq \delta \leq \alpha\}$. $\langle$obs. (3.18) p. 19 $\in$ [1]$\rangle$

- *Eratosthenes's Prime Sieve*: $\langle$rem. (3.20) p. 20 $\in$ [1]$\rangle$
  1) Fill the seive with the unmarked numbers: $\{a \in \mathbb{Z} \mid a \geq 2\}$
  2) To mark the next prime p_i:
     Mark lowest unmarked number p_i and
     remove all unmarked multipliers of p_i in the seive.

Rational Numbers

- **The set $\mathbb{Q}$ of *rational numbers*** $\overset{def}{=} \{\frac{a}{s} \mid a, s \in \mathbb{Z}, s \neq 0\}$. ⟨(4.1) p. 23 ∈ [1]⟩
- $\frac{a}{s} \overset{def}{=} as^{-1}$. ⟨(4.1) p. 23 ∈ [1]⟩
- $\mathbb{Z} \subseteq \mathbb{Q}$, since: $\forall a \in \mathbb{Z} : \frac{a}{1} \in \mathbb{Q}$. ⟨(4.1) p. 23 ∈ [1]⟩
- $\forall t \in \mathbb{Z}\backslash\{0\} : \frac{at}{st} = \frac{a}{s}$. ⟨(4.1.1) p. 23 ∈ [1]⟩
- $a, b \in \mathbb{Q} \Rightarrow a + b, a \cdot b \in \mathbb{Q}$:
  $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ ⟨(4.1.2) p. 23 ∈ [1]⟩
  $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ ⟨(4.1.3) p. 23 ∈ [1]⟩
- The *opposite number* for a fraction $\frac{a}{s}$ is $\frac{-a}{s}$:
  $-\frac{a}{s} = \frac{-a}{s}$. ⟨(4.1.4) p. 23 ∈ [1]⟩
- $0 = \frac{0}{1} = \frac{0}{s}, s \neq 0$. ⟨(4.1) p. 23 ∈ [1]⟩
- $1 = \frac{1}{1} = \frac{s}{s}, s \neq 0$. ⟨(4.1) p. 23 ∈ [1]⟩
- The *reciprocal* for a fraction $\frac{a}{s} \neq 0$ is $\frac{s}{a}$:
  $(\frac{a}{s})^{-1} = \frac{s}{a}$. ⟨(4.1) p. 23 ∈ [1]⟩
- All the usual *simple calculation rules* hold for *fractions*. ⟨(4.1) p. 23 ∈ [1]⟩
- Any fraction $\frac{a}{s}$ can be written $\frac{a'}{s'}$ with *positive denominator* s' and with a' and s' *primic* (i.e.: $\frac{a'}{s'}$ unshortenable). ⟨obs. (4.2) p. 23 ∈ [1]⟩
- For r fractions $\frac{a_1}{s_1}, \ldots, \frac{a_r}{s_r}$ we can always rewrite with a *common denominator*: $s_1 \cdot \cdots \cdot s_r$. ⟨obs. (4.2) p. 24 ∈ [1]⟩
- **The *Farey fractions*** of order $N \overset{def}{=}$
  $\{\frac{a}{s} \mid a, s \in \mathbb{Z}, 1 \leq s \leq N\}$. ⟨(4.3) p. 24 ∈ [1]⟩

1.3 Complex Numbers

- **The set $\mathbb{C}$ of *complex numbers*** $\overset{def}{=}$ the set $\mathbb{R}^2$ of pairs (a,b) with:

  $(a,b)+(c,d) \overset{def}{=} (a+c, b+d)$ ⟨(5.2.1) p. 25 ∈ [1]⟩
  $(a,b)\cdot(c,d) \overset{def}{=} (ac-bd, ad+bc)$ ⟨(5.2.1) p. 25 ∈ [1]⟩

  $\mathbb{C}$ is also called the *real area.* ⟨(5.2) p. 25 ∈ [1]⟩

- The rules for *addition* and *multiplication* hold for numbers in $\mathbb{C}$, but *not* the rules for *order.* ⟨(5.1) p. 25 ∈ [1]⟩

- Neutral element for addition: $(0,0)$ ⟨(5.2) p. 25 ∈ [1]⟩
  Neutral element for multiplication: $(1,0)$ ⟨(5.2) p. 25 ∈ [1]⟩
  Inverse element for addition of (a,b): $-(a,b)=(-a,-b)$ ⟨(5.2) p. 25 ∈ [1]⟩

- $\mathbb{R}\subseteq\mathbb{C}$ by: $a\mapsto(a,0):\mathbb{R}\to\mathbb{C}$, which is *injective* and thus gives a *bijective correspondence* between the real numbers and the complex numbers of the form $(a,0)$.
  All rules of calculation are the same for $\mathbb{R}$ when considered elements of $\mathbb{C}$.
  ⟨(5.2) p. 25 ∈ [1]⟩

- **The *imaginary unit*** $\overset{def}{=} (0,1)\in\mathbb{C}$, ⟨(5.2) p. 25 ∈ [1]⟩

- $(1,0)$ and $(0,1)$ is the *canonical basis* for $\mathbb{R}^2$ and gives the unique representation: $z=a+ib$ for a $z\in\mathbb{C}$, where a is the ***real part* of** z and b is the ***imaginary part* of** z.
  ⟨(5.2) p. 25 ∈ [1]⟩

- For $z=a+ib, z\in\mathbb{C}$ we define:
  Modulus $|z|$**, a.k.a. the *numerical value*, a.k.a. the *norm*** $\overset{def}{=}$ $|z|=\sqrt{a^2+b^2}$. ⟨(5.3) p. 25 ∈ [1]⟩
  Corresponds to the *Euclidean norm* of $(a,b)\in\mathbb{R}^2$.
  $|0|=0$, $z\neq 0\Rightarrow|z|>0$.

- **The *conjugated*** $\overline{z}$ **of** $z\in C$**,** $z=a+ib \overset{def}{=} \overline{z}=a-bi$. ⟨(5.3) p. 25 ∈ [1]⟩

- $z=\overline{z}\Leftrightarrow z\in\mathbb{R}$. ⟨(5.3) p. 25 ∈ [1]⟩

- $\overline{\overline{z}}=z$
  $z\overline{z}=|z|^2$
  $\overline{z+w}=\overline{z}+\overline{w}$
  $\overline{zw}=\overline{z}\cdot\overline{w}$
  ⟨(5.3) p. 26 ∈ [1]⟩

- **For** $z\neq 0$**:** $z^{-1}\overset{def}{=}\frac{\overline{z}}{|z|^2}=\frac{a-ib}{a^2+b^2}$, and $z^{-1}z=1$. ⟨(5.3) p. 25 ∈ [1]⟩

- Any complex number $z\neq 0$ defines ***a halfline*** l_z **from** 0 **through** z.
  l_1 is the *positive real axis.* ⟨(5.4) p. 26 ∈ [1]⟩

- $\theta\in\mathbb{R}$ **is an *argument* for** $z\in\mathbb{C}, z\neq 0$ $\overset{def}{=}$
  θ is the angle from l_1 to l_z. ⟨(5.4) p. 26 ∈ [1]⟩

- If θ is an argument for $z\in\mathbb{C}, z\neq 0$, then *the other arguments* for z are: $\{\theta+2\pi q\mid q\in\mathbb{Z}\}$. ⟨(5.4) p. 26 ∈ [1]⟩
  So there exists *exactly one* argument θ such that $0\leq\theta\leq 2\pi$ and *exactly one* argument θ such that $-\pi<\theta\leq\pi$. ⟨(5.4) p. 26 ∈ [1]⟩

- For $z, w \in \mathbb{C}$, $z, w \neq 0$ with arguments θ_z, θ_w respectively:
  $|z \cdot w| = |z||w|$ and $\theta_z + \theta_w$ is an argument for $z \cdot w$. ⟨(5.5) p. 26 ∈ [1]⟩
- **The *complex units* $\mathbb{U}$ a.k.a. the *complex signs*** $\stackrel{def}{=}$
  $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. $\mathbb{U}$ is the *unit circle* on $\mathbb{C}$.
  $\mathbb{U}$ is all $e^{i\theta} = \cos\theta + i\sin\theta$, where θ is an argument. ⟨(5.6) p. 27 ∈ [1]⟩
- For $z \in \mathbb{C}, z \neq 0$ we have $|z| > 0$ and $\frac{z}{|z|}$ is a *unit* of the form $e^{i\theta}$, where $\theta \in \mathbb{R}$ is an argument for z. ⟨(5.6) p. 27 ∈ [1]⟩
  We have $z = |z|\frac{z}{|z|} = re^{i\theta}$, where $r \in \mathbb{R}_+$.
  So z is a product of a *real positive number* and a *unit.*
- For $z, w \in \mathbb{C}, z = re^{i\theta}, w = se^{i\phi}$ we have:
  $zw = rse^{i\theta}e^{i\phi} = rse^{i(\theta+\phi)}$. ⟨(5.6) p. 27 ∈ [1]⟩
- $e^{i\theta}e^{i\phi} = e^{i(\theta+\phi)}$ written in coordinates are the *addition formulas*:
  $\cos(\theta+\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$
  $\sin(\theta+\phi) = \sin\theta\cos\phi + \cos\theta\sin\phi$ ⟨(5.6) p. 27 ∈ [1]⟩
- $\forall n \in \mathbb{N}$: There are *exactly* n solutions to the equation $z^n = 1$. These are: $\{e^{2\pi i a/n} \mid a \in \{0, \ldots, n-1\}\}$ and are called **the *n'th unit roots***.
  ⟨ex. (5.7) p. 27 ∈ [1]⟩

1.4 Remainder Classes and Congruence

Premises: $n \in \mathbb{N}$.

- $x, y \in \mathbb{Z}$ **are *congruent modulo* n:** $x \equiv y \pmod{n} \stackrel{def}{=} n|(x-y)$. ⟨(6.6) p. 31 ∈ [1]⟩
  Congruence is an *equivalence relation* on $\mathbb{Z}$.
- **The *remainer class* $[a]$ *modulo* n, a.k.a.** $[a]_n \stackrel{def}{=}$ the *equivalence class* of a w.r.t. *congruence modulo* n.
- **The *quotient set*** $\mathbb{Z}/n\mathbb{Z} \stackrel{def}{=} \{[a]_n \mid a \in \mathbb{Z}\}$.
  I.e. the *remainder classes* $[a]_n$ w.r.t *congruence modulo* n form $\mathbb{Z}/n\mathbb{Z}$.
  A.k.a. $\mathbb{Z}/n$, $\mathbb{Z}_n$ or $\mathbb{Z}/\equiv$. ⟨(6.6) p. 31 ∈ [1]⟩
- The numbers $r \in \mathbb{Z}$ satisfying: $a = qn + r$, where $a, q \in \mathbb{Z}$ (as in the *division theorem*) are the numbers which are *congruent* with a modulo n, i.e. the elements of $[a]_n$. ⟨(6.6 p. 31-32 ∈ [1]⟩
  There is thus *exactly one principal remainder* $r \in [a]_n$ satisfying $0 \leq r < n$.
- There are n *remainder classes* $[a]_n$ and n *principal remainders* from division by n: $[0], [1], \ldots, [n-1]$. ⟨(6.6) p. 32 ∈ [1]⟩

1.5 Addition and Multiplication of Remainder Classes

Premises: $n \in \mathbb{N}$. **A, B are *remainder classes* modulo n.**

- $\mathbf{0} = \mathbf{0}_n \stackrel{def}{=} [0]_n$. ⟨(6.6) p. 32 ∈ [1]⟩
- $\mathbf{1} = \mathbf{1}_n \stackrel{def}{=} [1]_n$. ⟨(6.6) p. 32 ∈ [1]⟩
- **Addition:** $A + B \stackrel{def}{=} [a+b]$, where we have *chosen* some $a \in A, b \in B$. ⟨(6.8.1) p. 32 ∈ [1]⟩
- **Multiplication:** $A \cdot B \stackrel{def}{=} [ab]$, where we have *chosen* some $a \in A, b \in B$. ⟨(6.8.1) p. 32 ∈ [1]⟩
- **Negation:** $-A \stackrel{def}{=} [-a]$, where we have *chosen* some $a \in A$. ⟨(6.8) p. 32 ∈ [1]⟩
- The *results* of *addition*, *multiplication* and *negation* are *independent* of the *choices* of $a \in A, b \in B$. ⟨(6.8) p. 32 ∈ [1]⟩
- The following calculation rules apply to *remainder classes* A, B and C modulo n: ⟨(6.9) p. 32 ∈ [1]⟩

$A + B = B + A$	a0
$A + (B + C) = (A + B) + C$	a1
$A + \mathbf{0} = \mathbf{0} + A = A$	a2
$A + (-A) = (-A) + A = \mathbf{0}$	a3
$AB = BA$	m0
$A(BC) = (AB)C$	m1
$A\mathbf{1} = \mathbf{1}A = A$	m2
$[a][a]^{-1} = [a]^{-1}[a] = \mathbf{1}$, if a is *primic* with n	m3
$A(B + C) = AB + AC$	am

1.6 Primic and Invertible Remainder Classes and Misc

- **A *modulo* 11 *congruence* for an** $a \in \mathbb{N}$ written in the *decimal numbering system with the digits* $a_k \cdots a_0$, *i.e.* $a = a_k 10^k + \cdots + a_1 10 + a_0$:
  $a \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \pmod{11}$. ⟨ex. (6.10) p. 33-34 ∈ [1]⟩
  In particular, a is *divisible* by 11 ⇔ the *right-hand side* is divisible by 11.

- **A *primic remainder class* modulo** $n \overset{def}{=}$
  a remainder class $[a]$ modulo n where a *primic* with n.
  All elements of a primic remainder class are *primic* with n,
  so the *choice* of element *does not matter*.
  The primic remainder classes are those of the form:
  $[r]$ for $0 \leq r < n$ and $gcd(r, n) = 1$. ⟨(6.11) p. 34 ∈ [1]⟩

- ***Euler's ϕ-function,*** $\phi : \mathbb{N} \to \mathbb{Z} \overset{def}{=}$
  $\phi(n) =$ *number* of *primic remainder classes* modulo n. ⟨(6.11) p. 34 ∈ [1]⟩

- $\mathbf{1}$ is a *primic remainder class.*

- $\mathbf{0}$ is *not* a primic remainder class *modulo* $n > 1$, but
  $\mathbf{0}$ *is* a primic remainder class *modulo* 1.
  So $\mathbf{0}_1 = \mathbf{1}_1$ and $\phi(1) = 1$.

- **An *invertible remainder class*** A **modulo** $n \overset{def}{=}$
  $\exists A^{-1} : A^{-1}A = \mathbf{1}$ modulo n. ⟨(6.11) p. 34 ∈ [1]⟩
  Such an A^{-1} is *unique* and is called the *inverse class* of A.

- A remainder class A is *invertible* ⇔ A is *primic.* ⟨(6.11) p. 34 ∈ [1]⟩

- $(\mathbb{Z}/n)^* \overset{def}{=}$
  the set of *all primic remainder classes* as a *subset* of $\mathbb{Z}/n$. ⟨(6.11 p. 34 ∈ [1]⟩

- Modulo 10 the classes:
  $[1], [3], [7], [9]$ are *primic*. E.g.: $3 \cdot 7 = 21 \equiv 1 \pmod{10}$. ⟨ex. (6.12) p. 35 ∈ [1]⟩
  Hint: Searching for remainder classes *primic modulo* n means searching for products $h \cdot k \in \{1, n+1, 2n+1, 3n+1, \ldots\}$.
  E.g. modulo 9 it's: $1, 10, 19, 28, 37, \ldots$ (the "9-table + 1").

- For remainder classes modulo a *prime* p:
  All remander classes modulo p *except* $[0]$ are *invertible.* ⟨ex. (6.13) p. 35 ∈ [1]⟩
  So $\phi(p) = p - 1$, for p *prime.*

- For remainder classes modulo a *prime power* p^r:
  All remander classes modulo p^r *except*
  $\{bp \mid b \in \{1, \ldots, p^{r-1}\}\}$ are *invertible.*
  Notice that we use p^r for 0: $p^r \equiv 0 \pmod{p^r}$. ⟨ex. (6.13) p. 35 ∈ [1]⟩
  So $\phi(p^r) = p^r - p^{r-1} = p^{(r-1)}(p-1)$, for p *prime*, $r \in \mathbb{N}$.

- Let $n = n_1 \cdot \dots \cdot n_r$ be a *product* of *pairwise primic* $n_i \in \mathbb{N}$:
  - *Chinese Remainder Class Theorem*: (special case of *Structure Thm.*)
    For *any tuple* $(a_1, \dots, a_r)$ of *integers* a_i:
    The *system* of *congruences*:
    $x \equiv a_1 \pmod{n_1}, \dots, x \equiv a_r \pmod{n_r}$ has *solutions* $x \in \mathbb{Z}$
    and these solutions form *one remainder class* modulo n.
    ⟨(6.14) p. 35 ∈ [1]⟩
    Equivalently: There is a *well-defined bijective map*
    $\mathbb{Z}/n \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ given by
    $[x]_n \mapsto ([x]_{n_1}, \dots, [x]_{n_r})$ for $x \in \mathbb{Z}$. ⟨(6.14.1) p. 35 ∈ [1]⟩
  - $[a]_n$ is a *primic remainder class* $\Leftrightarrow$
    $\forall i \in \{1, \dots, r\} : [a]_{n_i}$ *primic remainder class.* ⟨(6.15) p. 36 ∈ [1]⟩
  - By the above 2 theorems, the *primic remaninder classes* modulo n *correspond* to r*-tuples* of *primic remainder classes.* ⟨(6.15) p. 36 ∈ [1]⟩
  - $\phi(n) = \phi(n_1) \cdot \dots \cdot \phi(n_r)$. ⟨(6.15.1) p. 36 ∈ [1]⟩
- For a *prime resolution* $n = p_1^{\nu_1} \cdot \dots \cdot p_r^{\nu_r}$, where the p_i are *distinct*:
  $\phi(n) = \phi(p_1^{\nu_1}) \cdot \dots \cdot \phi(p_r^{\nu_r})$ and $\phi(p_i^{\nu_i}) = p_i^{(\nu_i - 1)}(p_i - 1)$. ⟨(6.15.2) p. 36 ∈ [1]⟩

2 Groups

2.1 Groups - The Creation

Premises: G ***set***.

- **A *group*** $\stackrel{def}{=}$ a *set* G along with a *composition* $(x, y) \mapsto x * y : G \times G \to G$, where the following hold:

  1) *Associativity* $\quad (x * y) * z = x * (y * z)$
  2) There *exists* a *neutral element* e in G $\quad e * x = x * e = x$
  3) There *exists* an *inverse element* x^{-1} in G $\quad x^{-1} * x = x * x^{-1} = e$

  ⟨def (1.2) p. 39 ∈ [1]⟩
- **A *commutative group* / *Abelian group*** $\stackrel{def}{=}$ a *group* where *commutativity* holds: $x * y = y * x$ ⟨def (1.2) p. 40 ∈ [1]⟩
- **The *order* $|G|$ of a *group* G** $\stackrel{def}{=}$ the *number of elements* in G. ⟨def (1.2) p. 40 ∈ [1]⟩
- ***Multiplicative notation*** $\stackrel{def}{=}$ use the *symbol* $\cdot$ for $*$, where $x \cdot y$ is called the *product* of x and y ⟨(1.3) p. 40 ∈ [1]⟩
- ***Additive notation*** $\stackrel{def}{=}$ use the *symbol* $+$ for $*$, where $x + y$ is called the *sum* of x and y. The *inverse element* of x is then denoted $-x$. This notation is *only used* for *commutative groups*. ⟨(1.3) p. 40 ∈ [1]⟩
- ***Map notation*** $\stackrel{def}{=}$ the composition is $(x, y) \mapsto f(x, y)$. ⟨(1.3) p. 40 ∈ [1]⟩

2.2 Invertible Elements

Premises: S ***set* with composition** $*$.
$*$ **obeys the rules for *associativity* and *neutral element* (denoted e), but the rules about *inverse element* does *not always* hold**.

- $x \in S$ **is an *invertible element*** $\stackrel{def}{=}$ there *exists* an $x^{-1} \in S$ such that: $x^{-1} * x = x * x^{-1} = e$.
  There is *at most one* such element x^{-1}. ⟨(1.4) p. 41 ∈ [1]⟩
- The *neutral element* e is *always invertible* and: $e = e^{-1}$. ⟨(1.4.2) p. 41 ∈ [1]⟩
- For $x, y \in S$ *invertible*: $z = x * y$ is *invertible* and $z^{-1} = (x * y)^{-1} = y^{-1} * x^{-1}$. ⟨(1.4.3) p. 41 ∈ [1]⟩
- For $x \in S$ *invertible*: $(x^{-1})^{-1} = x$. ⟨(1.4.4) p. 41 ∈ [1]⟩
- *All elements* of a *group* are *invertible* and all these rules hold:

  $$\begin{aligned} e &= e^{-1} \\ (x * y)^{-1} &= y^{-1} * x^{-1} \\ (x^{-1})^{-1} &= x \end{aligned}$$

  ⟨(1.4) p. 41 ∈ [1]⟩

2.3 Derived Group Concepts

- ***Stable subset*** H of a *set* S with a *composition* $(x,y) \mapsto x * y \overset{def}{=}$ $x, y \in H \Rightarrow x * y \in H$. ⟨def. (1.5) p. 41 ∈ [1]⟩
  The *composition* in S defines a *composition* in H by *restriction*.

- Let S be a *set* with an *associative composition* $*$ and a *neutral element* e.
  The set $S^* \overset{def}{=}$ the set of *all invertible elements* of S.
  $S^* \subseteq S$ is *stable*.
  S^* is a *group*. ⟨(1.5) p. 41 ∈ [1]⟩

- ***Subgroup*** H of the *group* $G \overset{def}{=}$ a *subset* H of G where:
  1) H is a *stable subset* of G
  2) The *neutral element* of G *lies in* H
  3) $x \in H \Rightarrow x^{-1} \in H$

  ⟨(1.6) p. 42 ∈ [1]⟩

- A *subgroup* is a *group* in itself. ⟨(1.6) p. 42 ∈ [1]⟩

- **The *trivial subgroups* of** $G \overset{def}{=} \{e\}$ and G. ⟨(3.1) p. 69 ∈ [1]⟩

- **A *genuine subgroup*** H **of** $G \overset{def}{=} H \underset{subgroup}{\subset} G$ (i.e. $G \neq H$).
  ⟨(3.1) p. 69 ∈ [1]⟩

- If G is a *finite group* and $H \subseteq G$ is a *non-empty* and *stable* subset, then H is a *subgroup* of G. ⟨exc. 4 p. 51 ∈ [1]⟩

- ***Product group*** $G_1 \times G_2$ of G_1 and $G_2 \overset{def}{=}$ ⟨(3.19) p. 76 ∈ [1]⟩
  $G_1 \times G_2$ with *composition*: $(g_1, g_2)(h_1, h_2) \mapsto (g_1 h_1, g_2 h_2)$. This is a *group*.

2.4 Well-known Groups

- **The *trivial group*** $C_1 \overset{def}{=} (\{e\}, *)$, where $e * e = e$. ⟨(1.7) p. 42 ∈ [1]⟩

- ***Additive groups* of *numbers*** $(\mathbb{L}, +) \overset{def}{=}$
  A *set of numbers* with *addition* forming a *group*. ⟨(1.8) p. 42 ∈ [1]⟩
  E.g. $(\mathbb{R}, +)$ (a.k.a. $\mathbb{R}^+$, not to be confused with the positive reals $\mathbb{R}_+$).

- ***Multiplicative groups* of *numbers*** $(\mathbb{L}, \cdot) \overset{def}{=}$
  A *set of numbers* with *multiplication* forming a *group*. ⟨(1.9) p. 42 ∈ [1]⟩
  E.g. $(\mathbb{R}\backslash\{0\}, \cdot)$ is a *group* (a.k.a. $\mathbb{R}^*$). But $(\mathbb{R}, \cdot)$ is *not* a group.

- $\mathbb{R}^*_+$ (the *positive reals*) is a *subgroup* of $\mathbb{R}^*$. ⟨(1.9) p. 42 ∈ [1]⟩

- *Multiplicative groups*: $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$, $\mathbb{U}$ (the *complex units*), $C_2 \overset{def}{=} (\{-1, 1\}, \cdot)$ ⟨(1.9) p. 42 ∈ [1]⟩

- *Subgroup relations*: $C_2 \subseteq \mathbb{Q}^* \subseteq \mathbb{R}^* \subseteq \mathbb{C}^*$, $\mathbb{U} \subseteq \mathbb{C}^*$. ⟨(1.9) p. 42 ∈ [1]⟩

- $\mathbb{Z}\backslash\{0\}$ is a *stable subset* of $\mathbb{Q}^*$, but *not a subgroup*!
  Because: $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$. ⟨(1.9) p. 42 ∈ [1]⟩

- Groups of *order* 2 (like C_2) are always given by:

*	e	u
e	e	u
u	u	e

The names e and u can stand for "even" and "uneven". ⟨(1.10) p. 43 ∈ [1]⟩
The table is exactly the *parity rules* for *addition* of *whole numbers*.

- ***Remainder class commutative additive group*** $\mathbb{Z}/n$ **(a.k.a.** $\mathbb{Z}/n\mathbb{Z}$**) for a given** $n \in \mathbb{N}$ $\stackrel{def}{=}$
the n remainder classes $\{[0],[1],\dots,[n-1]\}$ modulo n with *addition*.
$\mathbb{Z}/n$ has *order* n. ⟨(1.11) p. 43 ∈ [1]⟩

- ***Primic remainder class commutative multiplicative group*** $(\mathbb{Z}/n)^*$ **for a given** $n \in \mathbb{N}$ $\stackrel{def}{=}$
the primic remainder classes modulo n:
$\{[r]_n \mid r \text{ primic with } n\}$ with *multiplication*.
The *order* of $(\mathbb{Z}/n)^*$ is the *number* of r, where $0 \le r < n$ and $gcd(r,n) = 1$.
This number is denoted by *Euler's ϕ-function* $\phi(n)$.
So $|(\mathbb{Z}/n)^*| = \phi(n)$. ⟨(1.12) p. 43-44 ∈ [1]⟩

- **The *Cyclic Group*** C_n **of *order*** n $\stackrel{def}{=}$
$\{z \in \mathbb{Z} \mid z^n = 1\}$, i.e. the set of the n'th *unit roots*.
These are: $\{e^{2\pi ia/n} \mid a \in \{0,\dots,n-1\}\}$.
Subgroup relations: $C_n \subseteq \mathbb{U}$. ⟨(1.13) p. 44 ∈ [1]⟩
For $a = 1$ we define $\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$.
We have: $C_n = \{\zeta_n^a \mid a \in \{0,\dots,n-1\}\}$.
Product: $\zeta_n^a \cdot \zeta_n^b = \zeta_n^{a+b}$, where a and b can be *modulo* n.
So, multiplication in C_n *corresponds* to *addition of exponents* modulo n.

- $C_8 = \{\zeta_8^a \mid a \in \{0,\dots,n-1\}\}$.
We define: $\xi = \zeta_8^3$ and we get:
$C_8 = \{\xi^a \mid a \in \{0,\dots,n-1\}\}$. ⟨(1.13) p. 44 ∈ [1]⟩

- $C_3 = \{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\}$. ⟨ex. (1.14) p. 45 ∈ [1]⟩
z^3 can be rewritten to $(z-1)(z^2+z+1) = 0$.

- $C_4 = \{1, i, -1, -i\}$. ⟨ex. (1.14) p. 45 ∈ [1]⟩

- *Vector spaces*: ⟨(1.15) p. 45 ∈ [1]⟩
$\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$ with *vector addition* are *commutative groups*.

- Let X be a *set*.
The *Full Transformation Group* for X**, a.k.a. the *Full Permutation Group* for** X**, denoted** S_X **or** $Perm(X)$ $\stackrel{def}{=}$
the group of all *bijective maps* $f : X \to X$ with *function composition*:
$(f,g) \mapsto f \circ g$. ⟨(1.16) p. 45-46 ∈ [1]⟩
The *identity map* id_X (a.k.a. 1_X) is the *neutral element*.
The *inverse function* f^{-1} is the *inverse element* of f.
Multiplicative notation is often used for this group, i.e. fg for $f \circ g$.

- **The *Additive Matrix Group*** $Mat_{m,p}(\cdot)$ **of** $m \times p$ **matrices** $\stackrel{def}{=}$
the *commutative group* of $m \times p$ matrices with *matrix addition*.
Denoted: $Mat_{m,p}(\mathbb{Z})$,$Mat_{m,p}(\mathbb{Q})$,$Mat_{m,p}(\mathbb{R})$,$Mat_{m,p}(\mathbb{C})$.
We use $Mat_m(\cdot)$ for $Mat_{m,m}(\cdot)$. ⟨(1.17) p. 46 ∈ [1]⟩
We can identify $\mathbb{R}^{mp}$ with $Mat_{m,p}(\mathbb{R})$.

- **The *General Linear Group* $GL_n(\cdot)$ of *degree* n** $\stackrel{def}{=}$ ⟨(1.18) p. 46-47 ∈ [1]⟩
  the group of *invertible* $n \times n$ *matrices* with *matrix multiplication*.
  $GL_n(\mathbb{C}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{C}) \mid \det A \neq 0\}$.
  $GL_n(\mathbb{R}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{R}) \mid \det A \neq 0\}$.
  $GL_n(\mathbb{Q}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{Q}) \mid \det A \neq 0\}$.
  $GL_n(\mathbb{Z}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{Z}) \mid \det A \in \{-1, 1\}\}$. *Notice*: $\det A \in \{-1, 1\}$!
  Subgroup relations: $GL_n(\mathbb{Z}) \subseteq GL_n(\mathbb{Q}) \subseteq GL_n(\mathbb{R}) \subseteq GL_n(\mathbb{C})$.

- **The *Special Linear Group* $SL_n(\cdot)$ of *degree* n** $\stackrel{def}{=}$ ⟨(1.19) p. 47 ∈ [1]⟩
  the group of $n \times n$ *matrices* where the *determinant* is 1,
  with *matrix multiplication*.
  $SL_n(\mathbb{C}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{C}) \mid \det A = 1\}$.
  $SL_n(\mathbb{R}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{R}) \mid \det A = 1\}$.
  $SL_n(\mathbb{Q}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{Q}) \mid \det A = 1\}$.
  $SL_n(\mathbb{Z}) \stackrel{def}{=} \{A \in Mat_n(\mathbb{Z}) \mid \det A = 1\}$.
  Subgroup relations: $SL_n(\mathbb{Z}) \subseteq SL_n(\mathbb{Q}) \subseteq SL_n(\mathbb{R}) \subseteq SL_n(\mathbb{C})$ and
  $SL_n(\mathbb{Z}) \underset{normal}{\subseteq} GL_n(\mathbb{Z})$, $SL_n(\mathbb{Q}) \underset{normal}{\subseteq} GL_n(\mathbb{Q})$,
  $SL_n(\mathbb{R}) \underset{normal}{\subseteq} GL_n(\mathbb{R})$, $SL_n(\mathbb{C}) \underset{normal}{\subseteq} GL_n(\mathbb{C})$.

- **The *Orthogonal Group* $O_n(\mathbb{R})$ (a.k.a. $O(n)$) of *degree* n** $\stackrel{def}{=}$
  the group of *orthogonal functions* $f : \mathbb{R}^n \to \mathbb{R}^n$ with *function composition*.
  Note: $f : \mathbb{R}^n \to \mathbb{R}^n$ is *orthogonal* means that the *usual Euclidean distance* is *preserved*, i.e. if f is an *isometry* and it is *linear*.
  $f : \mathbb{R}^n \to \mathbb{R}^n$ *orthogonal* corresponds to $x \mapsto Ax$ for *orthogonal matrix* A.
  Function composition corresponds to *matrix multiplication* in this representation.
  Subgroup relations: $O_n(\mathbb{R}) \subseteq S_{\mathbb{R}}$, $O_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. ⟨(1.20) p. 47-48 ∈ [1]⟩
  $O_n(\mathbb{R})$ corresponds to the subgroup of *orthogonal matrices* in $GL_n(\mathbb{R})$.

- **The group of *actual movements (i.e. rotations)* $SO_n(\mathbb{R})$ of *degree* n** $\stackrel{def}{=}$
  The subgroup of $O_n(\mathbb{R})$ with *matrix determinant* 1.
  E.g. $SO_3(\mathbb{R}) = \{$ rotations about line through $(0, 0, 0)$ in $\mathbb{R}^3 \}$.
  Subgroup relations: $SO_n(\mathbb{R}) \underset{normal}{\subseteq} O_n(\mathbb{R})$.

- *About* $O_2(\mathbb{R})$: Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ correspond to $A = \begin{bmatrix} \mathrm{a} & \mathrm{c} \\ \mathrm{b} & \mathrm{d} \end{bmatrix}$.
  The following must hold: $(c, d) = (-b, a)$ or $(c, d) = (b, -a)$.
  A has one of these 2 forms: ⟨(1.20) p. 47-48 ∈ [1]⟩

$$\begin{aligned} R_\theta \ (\textit{notation in } [1] : D_\theta) &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in SO_2 \\ M_\theta \ (\textit{notation in } [1] : S_\theta) &= \begin{bmatrix} \sin\theta & -\cos\theta \\ \cos\theta & \sin\theta \end{bmatrix} \in O_2 \backslash SO_2 \end{aligned}$$

  R_θ is *rotation* with θ degrees.
  M_θ is *mirror* about $\vec{e} = (\cos \frac{1}{2}\theta, \sin \frac{1}{2}\theta)$.
  $\vec{e}$ is *eigen vector* for M_θ with *eigen value* 1.
  $\hat{\vec{e}} = (-\sin \frac{1}{2}\theta, \cos \frac{1}{2}\theta)$ is *eigen vector* for M_θ with *eigen value* -1.
  In the *orthonormal basis* $(\vec{e}, \hat{\vec{e}})$, M_θ is described by $\begin{bmatrix} 1 & 0 \\ 0 & \text{-1} \end{bmatrix}$.

- **Klein's Vier Group** V (Vier is German for 4) $\overset{def}{=}$
The *identity map* and the
3 *rotations* in $\mathbb{R}^3$ about *each of the axes* with *angle* π.
Subgroup relations: $V \subseteq O_3$. ⟨exc. 9 p. 51 ∈ [1]⟩

- **The *Dieder Group*** D_n **of degree** n $\overset{def}{=}$ ⟨(1.21) p. 48-50 ∈ [1]⟩
the group of *orthogonal maps* mapping *regular* n*-gons* in $\mathbb{R}^2$ such that the *corners* of *each* n*-gon* map to *corners* on the *same* n-gon.
Such maps are called *symmetries*.
An n-gon could be given by the corners $p_j = (\cos 2j\pi/n, \sin 2j\pi/n)$ for $j \in \{1, \ldots, n\}$. Indices are *modulo* n and $p_0 = p_n$.
Subgroup relations: $D_n \subseteq O_2(\mathbb{R})$.
There are $2n$ *symmetries* in D_n, i.e. D_n has *order* $2n$.
For $n \geq 3$ they are:

  - n *rotations* with *angles* $\{2j\pi/n \mid j \in \{0, \ldots, n-1\}\}$.
  - n *mirror transformations* through *axes passing* $(0,0)$ and *either a corner* or the *mid-point of an edge.*
    n *even*: The *mirror axes* either pass *2 corners or 2 edge mid-points.*
    n *uneven*: The *mirror axes* pass *a corner and an edge mid-point.*

  Let R be the *rotation* with the *angle* $2\pi/n$ and
  M be *mirroring* around the *first axis.*
  Then the symmetries are:
  $R^0, R^1, \ldots, R^{n-1}, M, RM, R^2M, \ldots, R^{n-1}M$. ⟨(1.21.1) p. 49 ∈ [1]⟩
  The following also hold:
  $R^0 = R^n = M^2 = id$, $MR = R^{-1}M$. ⟨(1.21.2) p. 49 ∈ [1]⟩
  These equations allow calculation using the R and M representations.
  Subgroup relations: $C_n \subseteq D_n$.

- **The *Quarternion Group*** Q_8 $\overset{def}{=}$ ⟨(1.22) p. 50 ∈ [1]⟩
the group $\{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ with *matrix multiplication*, where:
$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{i} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \mathbf{j} = \begin{bmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}.$
The following holds:
$i^2 = j^2 = k^2 = ijk = -1$
$ij = -ji = k$
$jk = -kj = i$
$ki = -ik = j$
Subgroup relations: $Q_8 \subseteq GL_2(\mathbb{C})$.

- **The *hexaeder group*** H $\overset{def}{=}$ ⟨ex. (7.11) p. 112 ∈ [1]⟩
The 24 *rotations* of $\mathbb{R}^3$ where a *hexaeder* with center $(0,0,0)$ is *invariant.*

2.5 Summaries

Table of known groups

Order	Various groups					Ref
1	$\mathbb{Z}/1 = C_1 = \{1\} = \{0\} = S_1$					
2	$\mathbb{Z}/2 = C_2 = \{\pm 1\} = D_1 = S_2$					
3	$\mathbb{Z}/3 = C_3$					
4	$\mathbb{Z}/4 = C_4 = (\mathbb{Z}/10)^* = (\mathbb{Z}/5)^*$	$V = C_2 \times C_2$				(7.25)
	$= (\mathbb{Z}/8)^*$	$= D_2 = (\mathbb{Z}/12)^*$				
5	$\mathbb{Z}/5 = C_5$					
6	$\mathbb{Z}/6 = C_6 = C_2 \times C_3 = (\mathbb{Z}/7)^*$	$D_3 = S_3$				(8.12)
7	$\mathbb{Z}/7 = C_7$					
8	$\mathbb{Z}/8 = C_8$	$C_2 \times C_2 \times C_2$	$C_4 \times C_2$	D_4	Q_8	
9	$\mathbb{Z}/9 = C_9$	$C_3 \times C_3$				(7.25), struct thm.
10	$\mathbb{Z}/10 = C_{10}$	D_5				(8.12)
11	$\mathbb{Z}/11 = C_{11}$					
12	$\mathbb{Z}/12 = C_{12}$	D_6	more?			

Until order 11, these are *all* groups.

Example of analyzing groups

⟨ex. (4.12) p. 83 ∈ [1]⟩

Showing that there are exactly 2 groups of order 6: (FIXME: this proof is wrong!)

1. $g^2 = e$ cannot hold for all $g \in G$.
   Otherwise $(g_2 g_1) = (g_2 g_1)^{-1} = (g_1 g_2)^{-1} = (g_1 g_2)$.
   $\{e, g_1, g_2\}$, 4 different elements forms a subgroup, contradiction.
2. Assume $\sigma \in G$ has order 3. $H = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$. Order 3.
   Assume $\tau \in G$ has order 3. $G = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$.

Showing how many groups of order 8 there are:

The structure theorem says that these 3 different groups are the *only commutative groups*: $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$.

Showing that there is at most 2 non-abelian groups of order 8. Assume G is non-abelian.

$\exists a \in G : ord(a) = 4$, since if there was an element a' with order 8 (then $\langle a' \rangle = G$ would be cyclic and thus abelian) and if all elements had order 2 it would also be abelian.

So $\langle a \rangle$ has index $8/4 = 2$ and is thus *normal* in G. Take a $b \in G \backslash \{a\}$. $G = \langle a \rangle \cup \langle a \rangle b$. $b^2 \langle a \rangle = (b\langle a \rangle)^2 = \langle a \rangle$, so $b^2 \in \langle a \rangle = \{e, a, a^2, a^3\}$. b^2 cannot have order 4 so $b^2 \notin \{a, a^3\}$.

Theorem: $ord(g^k) = \frac{ord(g)}{gcd(k, ord(g))}$.

Then $b^2 \in \{a^2, e\}$ (otherwise $ord(b) = 8$).

$bab^{-1} \in \langle a \rangle$ and $ord(bab^{-1}) = ord(a) = 4$. So $bab^{-1} \in \{a, a^3\}$. $bab^{-1} \neq a$, since otherwise $ba = ab$, which is impossible when G *not* abelian. So $ba = a^3 b$.

There are 2 possibilities:

1. $b^2 = e, a^4 = e, ba = a^3 b$.
2. $b^2 = a^2$, $a^4 = e$, $ba = a^3 b$. $(a^{k_1} b^{m_1})(a^{k_2} b^{m_2})$

Sets of Invertible Elements for Multiplication

- $\mathbb{N}^* = \{1\}$, $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$, $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$.
- $Mat_n(\mathbb{Z})^* = GL_n(\mathbb{Z})$.

Sets of Invertible Elements

- $(\text{"maps } X \to X\text{"}, \circ)^* = \{\text{bijective maps}\} = Perm(X)$.
- $(\mathbb{Z}/n)^* =$ *invertible remainder classes* modulo n.

Subgroups with Multiplication

- $\{1\} \subseteq \{\pm 1\} \subseteq \mathbb{Q}^* \subseteq \mathbb{R}^* \subseteq \mathbb{C}^*$.
- $\mathbb{U} \subseteq \mathbb{C}^*$, $\mathbb{Q}^*_+ \subseteq \mathbb{Q}^*$, $\mathbb{R}^*_+ \subseteq \mathbb{R}^*$, $\mathbb{Q}^*_+ \subseteq \mathbb{R}^*_+$.
- $C_n \subseteq \mathbb{C}^*$.

Subgroups with Addition

- $\mathbb{Z}^+ \subseteq \mathbb{Q}^+ \subseteq \mathbb{R}^+ \subseteq \mathbb{C}^+$.

2.6 Permutations

Premises: $X = \{x_1, \dots, x_n\}$ **a *finite set*,** S_X **the *permutation group* of** X.

- **The *symmetric group*** S_n **of *degree*** $n \overset{def}{=}$ S_X for $X = \{1, \dots, n\}$. ⟨(2.1) p. 53 ∈ [1]⟩

- S_n can be *identified* with S_X, by using the *numbers* in S_n as the *element indices* in S_X. ⟨(2.1) p. 53 ∈ [1]⟩

- S_X (and S_n) has *order* $n!$. ⟨(2.1) p. 53 ∈ [1]⟩

- Let the *permutation* σ be given by $\forall i \in \{1, \dots, n\} : \sigma(x_i) = y_i$.
  - **The *inverse permutation*** σ^{-1} is given by: $\forall i \in \{1, \dots, n\} : \sigma^{-1}(y_i) = x_i$. ⟨(2.2) p. 53-54 ∈ [1]⟩
  - *Table notation*: $\sigma = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \end{pmatrix}$. ⟨(2.2) p. 53-54 ∈ [1]⟩
    For a permutation, *all elements* of S_X must be present as columns.
    The *order of the columns* does *not matter.*
    Notation for inverse: $\sigma = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}$.
    For *multiplication*, the columns are ordered such that the order of the y_i are the same:
    $\tau\sigma = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ z_1 & z_2 & \cdots & z_n \end{pmatrix} \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ z_1 & z_2 & \cdots & z_n \end{pmatrix}$.
  - *Direct notation* for S_n: $\sigma = (\sigma(1), \sigma(2), \dots, \sigma(n))$.
    σ is a permutation when all $\sigma(i)$ are *distinct.* ⟨(2.4) p. 55 ∈ [1]⟩
  - *Graphical notation*: ⟨(2.5) p. 55 ∈ [1]⟩
    Elements x_i can be drawn as *points* in the plane, and permutations shown as *directed lines* from x_i to $\sigma(x_i)$.

- The permutation: $\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix} = (n, n-1, \dots, 2, 1)$ can be shown as a *mirror* of a *regular n-gon.* ⟨ex. (2.6) p. 55-56 ∈ [1]⟩

- **Two *permutations*** σ, τ ***commute*** $\overset{def}{=} \sigma\tau = \tau\sigma$.
  Permutations *do not commute in general* for $n \geq 3$. ⟨obs. (2.3) p. 54-55 ∈ [1]⟩

- For the *remainder classes* modulo n we identify $1, \dots, n$ with $[1], \dots, [n]$ $(= [0])$ and *permutations* in $\mathbb{Z}/n$ with permutations in S_n. ⟨ex. (2.7) p. 56 ∈ [1]⟩

- $x \in X$ **is *fixpoint* for the *permutation*** $\sigma \overset{def}{=}$ $\sigma(x) = x$. ⟨def. (2.8) p. 56 ∈ [1]⟩

- $x \in X$ **is *moved* by the *permutation*** $\sigma \overset{def}{=}$ $\sigma(x) \neq x$. ⟨def. (2.8) p. 56 ∈ [1]⟩

- **Two *permutations*** σ, μ **are *disjoint*** $\overset{def}{=}$ the set of elements *moved by* σ is *disjoint* from the set of elements *moved by* μ. ⟨def. (2.8) p. 56 ∈ [1]⟩

- Two *permutations* σ, μ are *disjoint* $\Rightarrow$
  σ, μ *commute.* ⟨def. (2.8) p. 56 $\in$ [1]⟩

- For p *different elements* $a_1, \ldots, a_p \in X$: ⟨(2.9) p. 56-57 $\in$ [1]⟩
  A p-*cycle* γ (a.k.a. a *cycle* of *length* γ) $\stackrel{def}{=}$
  a *permutation* $\gamma : X \to X$ where
  $\gamma(a_1) = a_2, \ldots, \gamma(a_{p-1}) = a_p, \gamma(a_p) = a_1$ and
  $\forall x \notin \{a_1, \ldots, a_p\} : \gamma(x) = x$. Furthermore:

  1. We use the ***cycle notation***: $\gamma = (a_1 \cdots a_p)$ (without any commas).
  2. The 1-*cycle* (a_1) is the *identity map.*
  3. *Any* of the a_i may be on the *first position*, because:
     $\gamma = (a_1 \cdots a_p) = (a_i a_{i+1} \cdots a_p a_1 \cdots a_{i-1})$. ⟨(2.9.1) p. 57 $\in$ [1]⟩

- *Note*: The set X *must be known* for the *cycle notation* to be *unambiguous.*
  ⟨ex. (2.10) p. 57-58 $\in$ [1]⟩

- By convention, a product of *no cycles* is the *identity map.*
  ⟨ex. (2.13) p. 59 $\in$ [1]⟩

- The *inverse* of a p-*cycle* is another p-*cycle*:
  $(a_1 \cdots a_p)^{-1} = (a_p a_{p-1} \cdots a_1)$. ⟨(2.9.2) p. 57 $\in$ [1]⟩

- **A *transposition* $\tau = (a_1 a_2)$** $\stackrel{def}{=}$
  a 2-*cycle.* It *swaps* a_1 and a_2. ⟨(2.9) p. 57 $\in$ [1]⟩

- Any p-*cycle* can be written as a *product* of $p-1$ *transpositions*:
  $(a_1 \cdots a_p) = (a_1 a_p)(a_1 a_{p-1}) \cdots (a_1 a_2)$. ⟨(2.9.3) p. 57 $\in$ [1]⟩
  Even as transpositions of the form (ax) for some *fixed* a (as seen above).

- **The *orbit* $B_a(\sigma)$ (a.k.a. B_a) ⟨ DK: Banen ⟩ determined by $a \in X$**
  for a *permutation* σ $\stackrel{def}{=}$
  $B_a(\sigma) = \{a_1, \ldots, a_p\}$ where the elements are the sequence:
  $a_1 = a, a_2 = \sigma(a_1), a_2 = \sigma(a_3), \ldots, a_{i+1} = \sigma(a_i), \ldots$. ⟨(2.11) p. 58 $\in$ [1]⟩

  - $p \in \mathbb{N}$ is the *unique* p such that $a_1, \ldots, a_p$ are *distinct* and $a_{p+1} = a_1$.
    The p **is the *length* of the orbit**.

- For *fixpoint* $a \in X$: $B_a = \{a\}$.
  I.e. *fixpoints* have *one-point orbits.* ⟨(2.11) p. 58 $\in$ [1]⟩

- *Any point* of an orbit determines the *same orbit.* ⟨(2.11) p. 58 $\in$ [1]⟩

- The *orbits* for a permutation σ make up
  a *partition* of X into *equivalence classes.* ⟨(2.11) p. 58 $\in$ [1]⟩

- **The p-*cycle derived from* an *orbit* $B_a(\sigma)$** $\stackrel{def}{=}$
  $\gamma = (a_1 \cdots a_p)$ for some $a_1 \in B_a(\sigma)$ and $a_{i+1} = \sigma(a_i)$. ⟨p. 58 $\in$ [1]⟩
  The choice of a_1 does not matter. We also have:

  1. $\forall x \in B_a(\sigma) : \sigma(x) = \gamma(x)$.
  2. For $x \notin B_a(\sigma) : x$ is a *fixpoint* for γ (but not for σ).

- *Cycle Theorem*: Let σ be a *permutation* of X with the *orbits* $B_1, \dots, B_m$ and the *derived cycles* $\gamma_1, \dots \gamma_m$. Then:
  $\sigma = \gamma_1 \cdots \gamma_m$. ⟨(2.12) p. 59 ∈ [1]⟩.
  $\gamma_1 \cdots \gamma_m$ is the ***cycle representation*** of σ.
  I.e.: Any *permutation* can be written as a *product of disjoint cycles.*

- Any *permutation* can be written as a *product* of *transpositions* of the form (ax) for some *fixed* a.
  For *transposition*: $(xy) = (ax)(ay)(ax)$. ⟨thm. (2.14) p. 59 ∈ [1]⟩

- Any *permutation* can be written as a *product* of *transpositions* of the form $(x_i x_{i+1})$ for some *ordering* $x_1, \dots, x_n$. ⟨thm. (2.14) (3) p. 59 ∈ [1]⟩

- $m(\sigma) \stackrel{def}{=}$ *number of oribits* for σ. ⟨(2.16) p. 60 ∈ [1]⟩

- $m_p(\sigma) \stackrel{def}{=}$ *number of orbits* of *length* p for σ. ⟨(2.16) p. 60 ∈ [1]⟩

- $m(\sigma) = \sum_p m_p(\sigma)$. ⟨(2.16.1) p. 61 ∈ [1]⟩

- $|G| = \sum_p p \cdot m_p(\sigma)$. ⟨(2.16.1) p. 61 ∈ [1]⟩

- **The *type* (a.k.a. *cycle type)* of the *permutation*** $\sigma \stackrel{def}{=}$
  The *sequence*: $m_1(\sigma), m_2(\sigma), m_3(\sigma), \dots$.
  Often written as a formal product: $1^{m_1} 2^{m_2} 3^{m_3} \cdots$. ⟨(2.16) p. 60-61 ∈ [1]⟩
  All *possible cycle types* in a group G correspond to *partitions* of the number $|X|$. ⟨p. 61 ∈ [1]⟩

  - The *cycle image* of σ: $\underbrace{(*)(*)\cdots(*)}_{m_1}\underbrace{(**)(**)\cdots(**)}_{m_2}\underbrace{(***)\cdots(***)}_{m_3}\cdots$.
    ⟨(2.16) p. 61 ∈ [1]⟩
  - $\sigma = \underbrace{(x_1)(x_2)\cdots(x_p)}_{m_1}\underbrace{(y_1 y_2)\cdots}_{m_2}\underbrace{(z_1 z_2 z_3)\cdots}_{m_3}\cdots$.

- $k = |G| - m(\sigma) = \sum(|B_i| - 1) = \sum_p m_p(\sigma)(p-1)$. ⟨(2.18) p. 62 ∈ [1]⟩
  σ can be written as a *product* of k *transpositions.*

- ***Sign* of a *permutation*** σ**:** $sign(\sigma) \stackrel{def}{=} (-1)^k$. ⟨(2.18) P. 62 ∈ [1]⟩

- For *transposition* τ: $k = 1$, $sign(\tau) = -1$. ⟨(2.18 p. 62 ∈ [1]⟩

- For *permutation* σ and *transposition* τ on *finite set* G:
  $m(\tau\sigma) = m(\sigma) \pm 1$. ⟨lemma (2.19) p. 62 ∈ [1]⟩

- For *permutations* σ, τ: $sign(\sigma\tau) = sign(\sigma) sign(\tau)$. ⟨thm. (2.20) p. 63 ∈ [1]⟩

- **A permutation** σ **is *even*** $\stackrel{def}{=}$ σ can be written as a product of an *even number of transpositions.* ⟨def. (2.21) p. 63 ∈ [1]⟩
  Note: *id* is *even* (0 transpositions by convention).

- **A permutation** σ **is *uneven*** $\stackrel{def}{=}$ σ can be written as a product of an *uneven number of transpositions.* ⟨def. (2.21) p. 63 ∈ [1]⟩

- $sign(\sigma) = \begin{cases} +1 & , \sigma \textit{ even, } k \textit{ even} \\ -1 & , \sigma \textit{ uneven, } k \textit{ uneven} \end{cases}$ ⟨cor. (2.22) p. 64 ∈ [1]⟩

- If the *finite set* X has *at least 2 elements*, then *half* of the *permutations* of $Perm(X)$ are *even.* ⟨cor. (2.22) p. 64 ∈ [1]⟩
- **The *Alternating Group* A_n of *degree* n** $\stackrel{def}{=}$
  The set of *even permutations*, which is a *subgroup* of S_n.
  Order: $|A_n| = \frac{1}{2}n!$ for $n \geq 2$.
  $A_1 = S_1 = C_1$. ⟨cor. (2.22) p. 64, def. (2.23) p. 64 ∈ [1]⟩
- Any *even permutation* in a *finite group* G can be written as a *product* of 3-*cycles.* ⟨(2.24) (1) p. 64 ∈ [1]⟩
  - The 3-cycles can even be chosen to be of the form (abx), for *fixed* $a, b \in G$ and $x \in G\backslash\{a, b\}$. ⟨(2.24) (2) p. 64 ∈ [1]⟩
  - Alternatively, the 3-cycles can be chosen to be of the form $(x_i x_{i+1} x_{i+2})$, for $i \in \{1, \ldots, n-2\}$, for some ordering $G = \{x_1, \ldots, x_n\}$. ⟨(2.24) (3) p. 64 ∈ [1]⟩
- Any permutation in the "15-game" which *starts* and *ends* with the blank piece in the *lower right corner* is *always even.* ⟨see p. 65-66 ∈ [1]⟩

2.7 Cyclic Groups

Premises: G **a *multiplicatively written* group**.

- **The *n'th order* g^n of an element** $g \in G \overset{def}{=}$ ⟨(3.2) p. 69 ∈ [1]⟩

  1. $n \in \mathbb{N} : g^n = g \cdot \cdots \cdot g$ with g occuring n times
  2. $n \in \mathbb{N} : g^{-n} = (g^{-1})^n$
  3. $g^0 = e$

  So $g^1 = g$ and g^{-1} is the *inverse* of g.

- Rules for *element powers*: ⟨(3.2) p. 69 ∈ [1]⟩

  (0) $g^1 = g$
  (1) $g^{p+n} = g^p g^n$
  (2) $g^{pn} = (g^p)^n$
  (3) $(gh)^n = g^n h^n$, if $gh = hg$

- Notation for n'th *power* of g for *additively written* group G :
  gn. ⟨(3.2) p. 69 ∈ [1]⟩

- Rules for *element powers additively written*: ⟨(3.2) p. 69-70 ∈ [1]⟩

  (0) $1 \cdot g = g$
  (1) $(p+n) \cdot g = pg + ng$
  (2) $(pn)g = p(ng)$
  (3) $n(g+h) = ng + nh$

  Rule (3) is *always valid*, since *additively written groups* are assumed to be *commutative*.

- **The *order* $|g|$ of an *element*** $g \in G \overset{def}{=}$ ⟨(3.4) p. 71 ∈ [1]⟩
  $(\forall n \in \mathbb{N} : g^n \neq e) \Rightarrow |g| = \infty$.
  Otherwise: $|g| = n$, where n is the *smallest* $n \in \mathbb{N}$ such that $g^n = e$.

- $|g| = 1 \Leftrightarrow g = e$. ⟨(3.4) p. 71 ∈ [1]⟩
  So neutral element has order 1 and all other elements g have $|g| > 1$.

- For some $g \in G$: **The *cyclic group* $\langle g \rangle$ *produced by*** $g \overset{def}{=}$
  $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\} \subseteq G$. ⟨thm. (3.5) p. 71 ∈ [1]⟩
  $\langle g \rangle$ is a *subgroup* of G and $|\langle g \rangle| = |g|$.
  I.e. the *element order* $|g|$ and the *group order* $|\langle g \rangle|$ are *equal*.

- For $|g| = |\langle g \rangle| = n$:

  - $g^i = g^j \Leftrightarrow (i \equiv j \pmod{n})$.
    I.e. *exponents* are *added modulo n*. ⟨thm. (3.5) p. 71, (3.7) p. 72 ∈ [1]⟩
  - $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ and the $e, g, g^2, \ldots, g^{n-1}$ are *distinct*.
    ⟨thm. (3.5) p. 71 ∈ [1]⟩
  - $\forall k \in \mathbb{Z} : g^k = e \Leftrightarrow n \mid k$. ⟨cor. (3.6) p. 72 ∈ [1]⟩

- For $|g| = |\langle g \rangle| = \infty$: $g^i = g^j \Leftrightarrow i = j$. ⟨(3.7) p. 72 ∈ [1]⟩

- G **is a *cyclic group*** $\overset{def}{=}$
  there *exists* an *element* $g \in G$ such that $\langle g \rangle = G$.
  Calculation in this group is done by *adding exponents.* ⟨(3.7) p. 72 ∈ [1]⟩

- For any $g \in G$ (where G *finite* and *cyclic*):
  $\langle g \rangle$ is a *cyclic subgroup* of G, called **the group *produced* by** g.
  ⟨(3.7) p. 72 ∈ [1]⟩

- *Any cyclic* group is *commutative.* ⟨(3.7) p. 72 ∈ [1]⟩

- The *order* of a *p-cycle* is *p.* ⟨ex. (3.14) p. 74 ∈ [1]⟩

- For $\sigma = \gamma_1 \cdots \gamma_r$ as a *product* of *disjoint cycles*:
  The *order* of σ is the *least common multiple* of the *orders* of the *cycles* $\gamma_1, \ldots, \gamma_r$. ⟨ex. (3.14) p. 74 ∈ [1]⟩

- The *element* $g \in G$ has *order* $n \Rightarrow g^t$ has *order* $\frac{n}{gcd(n,t)}$.
  Furthermore, $\langle g^t \rangle = \langle g^{gcd(t,n)} \rangle$. ⟨lemma (3.15) p. 74 ∈ [1]⟩

- For cyclic $G = \langle g \rangle$: *Any subgroup* $H \subseteq G$ is *cyclic.* ⟨thm. (3.16) p. 74 ∈ [1]⟩
  - If $|G| = \infty$ and $H \neq \{e\}$, then: $|H| = \infty$.
  - If $|G| = n$, then:
    * The *order* of H is *divisor* in the *order* of G.
    * For *any divisor* $d|n$ there *exists exactly one* subgroup S with $|S| = d$, namely the *cyclic subgroup* $\langle g^{n/d} \rangle$.
      I.e.: $\forall d \in \mathbb{N}, d|n : \exists! S \underset{subgroup}{\subseteq} G : |S| = d$.
    * For $n = kd$: g^k has *order* d.

- Given 2 *commuting* elements g, h (i.e. $gh = hg$) with *order* n, m,
  $|gh|$ is *divisor* in the *least common multiple* of n and m.
  If m, n are *primic*: $|gh| = mn$, otherwise $|gh| < nm$.
  ⟨lemma (3.17) ∈ [1]⟩
  Note: If g, h does *not* commute, then gh *may have infinite order.*
  ⟨ex. (3.18) p. 76 ∈ [1]⟩

- g and g^{-1} have the *same order.* ⟨ex. 8 p. 77 ∈ [1]⟩

- In the *product group* $G = G_1 \times G_2$: ⟨(3.19) p. 76 ∈ [1]⟩
  The *order* of $g = (g_1, g_2) \in G$ is
  the *least common multiple* of $|g_1|$ and $|g_2|$, if g_1 and g_2 have *finite orders.*

- For *cyclic groups* C_i, C_j of *finite orders* $|C_i| = n, |C_j| = m$: $|C_i \times C_j| = nm$.
  $C_i \times C_j$ is *cyclic* $\Leftrightarrow m$ and n are *primic.* ⟨thm. (3.20) p. 76 ∈ [1]⟩

Examples of Cyclic Groups

- For $\mathbb{Z}$ with *addition*: $\langle$ex. (3.8) p. 72 $\in$ [1]$\rangle$
  The *subgroup* of *all multiples* of $g \in \mathbb{Z} \overset{def}{=}$
  $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\} = g\mathbb{Z} = \mathbb{Z}g$.
  In particular:
  $\mathbb{Z}0 = \{0\}$. $\mathbb{Z}1 = \mathbb{Z}$. For $n > 1$, $\mathbb{Z}n$ is a *genuine subgroup* of $\mathbb{Z}$.

- $\mathbb{Z}/n$ is *cyclic* and produced by $[1]$. $\langle$ex. (3.9) p. 72 $\in$ [1]$\rangle$

- For p *prime*: $(\mathbb{Z}/p)^*$ is *cyclic*.
  E.g. $(\mathbb{Z}/7)^*$ is produced by $[3]$. $\langle$ex. (3.10) p. 73 $\in$ [1]$\rangle$

- C_n is *cyclic* and produced by $\zeta_n = e^{2\pi i/n}$. $\langle$ex. (3.11) p. 73 $\in$ [1]$\rangle$

- D_4 has *these cyclic subgroups*:
  $\langle 1 \rangle = \{1\}, \langle R \rangle, \langle R^2 \rangle, \langle M_i \rangle$ for $i \in \{1, 2, 3, 4\}$. $\langle$ex. (3.12) p. 72 $\in$ [1]$\rangle$

- Q_8 has *these cyclic subgroups*:
  $\langle 1 \rangle, \langle -1 \rangle, \langle i \rangle, \langle j \rangle, \langle k \rangle$. $\langle$ex. (3.13) p. 73 $\in$ [1]$\rangle$

2.8 Side classes

Premises: G ***group***

- ***Product composition*** AB **of** ***subsets*** A **and** B **of a** ***group*** $G \overset{def}{=}$ $AB = \{ab \mid a \in A \wedge b \in B\}$ ⟨(4.1) p. 79 ∈ [1]⟩
  Additively written: $A + B \overset{def}{=} \{a + b \mid a \in A \wedge b \in B\}$. ⟨obs. (4.4) p. 80 ∈ [1]⟩

- ***(Left) side classes*** gH ***modulo*** H**, where** H **is a** ***subgroup*** **of** $G \overset{def}{=}$
  For each $g \in G$ the *side class modulo* H is: $gH = \{gh \mid h \in H\}$.
  I.e. gH is a *side class* if there *exists* a $g \in G$ such that $gH = \{gh \mid h \in H\}$. ⟨p. 79 ∈ [1]⟩
  gH is also denoted: $[g]_H$ or just $[g]$. ⟨(4.4) p. 80 ∈ [1]⟩
  Additively written: $g + H = \{g + h \mid h \in H\}$. ⟨obs. (4.4) p. 80 ∈ [1]⟩
  Warning: Some books call this a *right side class.* ⟨(4.1) p. 79 ∈ [1]⟩

- ***Right side class*** $\overset{def}{=} Hg = \{hg \mid h \in H\}$. ⟨(4.13) p. 83-84 ∈ [1]⟩

- We have: $(gH)^{-1} = Hg$. ⟨(4.13) p. 84 ∈ [1]⟩
  I.e. the *inverse* of a *left side class* is a *right side class.*
  So $A \mapsto A^{-1}$ is a *bijective map* between *left* and *right side classes.*

- **The** ***index*** $|G : H|$ **of the** ***subgroup*** H **in** $G \overset{def}{=}$
  number of side classes modulo H.
  So *index* $|G : H|$ is the *same* for *right* and *left* side classes.
  For infinitely many side classes: $|G : H| = \infty$.
  For G *commutative* $gH = Hg$. ⟨(4.1) p. 79 ∈ [1]⟩

- *Lagrange's Index Theorem*: The *sideclasses modulo some given subgroup* H makes a *class division* of G, and two elements x, x' in G are in the *same sideclass* if and only if $x^{-1}x' \in H$.
  Each *sideclass* has the *same number of elements* as H, and the *number* of *sideclasses* $|G : H|$ is given by the formula:
  $|G| = |G : H| \cdot |H|$. ⟨4.2 p. 79 ∈ [1]⟩

- For a *subgroup* H of a *finite group* G:
  - $|H|$ and $|G : H|$ are *divisors* in $|G|$. ⟨cor. (4.3) p. 80 ∈ [1]⟩
  - $|G : H| = \frac{|G|}{|H|}$. ⟨(4.1) p. 79 ∈ [1]⟩

- Warning: There does *not* necessarily exist a *subgroup* of *order* d for *any* divisor d in $|G|$.
  E.g.: $|A_4| = 12$ and A_4 has *no subgroups* of order 6, ⟨ex. (4.18) p. 86 ∈ [1]⟩

- For *finite index* $|G : H| = r$: There are r side classes $g_1H, g_2H, \ldots, g_rH$ and G is the *disjoint union*: $G = g_1H \cup \cdots \cup g_rH$. ⟨(4.4) p. 80 ∈ [1]⟩

- For *finite* G: $\forall g \in G : |g| \mid |G|$. (*element order* is *divisor* in *group order*).
  In particular: $g^{|G|} = e$. ⟨cor. (4.7) p. 81 ∈ [1]⟩

- For $|G| = p$, where p is a *prime number*: $G = C_p$.
  More precisely: $\forall g \in G, g \neq e : \langle g \rangle = G$. $\langle$cor. (4.8) p. 81 $\in$ [1]$\rangle$

- Euler's Theorem: $\langle$thm. (4.9) p. 81 $\in$ [1]$\rangle$
  For $a \in \mathbb{Z}, n \in \mathbb{N} : gcd(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$.

- Fermat's small theorem: $\langle$(4.10) p. 82 $\in$ [1]$\rangle$
  For p *prime*: $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.

- **The *equivalence relation* $\sim$ "congruence modulo H"** $\stackrel{def}{=}$
  $x \sim x' \Leftrightarrow x$ and x' belongs to the *same side class*: $x \equiv x' \pmod{H}$.
  $x \equiv x' \pmod{H} \stackrel{def}{\Leftrightarrow} x^{-1}x' \in H$. A.k.a. "the *quotient* lies in H".
  $\langle$obs. (4.4) p. 80 $\in$ [1]$\rangle$
  Additively written: $x \equiv x' \pmod{H} \stackrel{def}{\Leftrightarrow} x' - x \in H$.

- Examples:

  - $|G : \{e\}| = |G|$ and $|G : G| = 1$.
    We can identify G and $G/\{e\}$. $\langle$ex. (4.5) p. 81 $\in$ [1]$\rangle$
  - For S_3 and $H = \langle \tau \rangle$, where $\tau = (12)$.
    $|S_3 : H| = 3$. $\langle$ex. (4.6) p. 81 $\in$ [1]$\rangle$
  - $n\mathbb{Z} \subseteq \mathbb{Z}$: $|\mathbb{Z} : n\mathbb{Z}| = n$. $\langle$ex. (4.5) p. 81 $\in$ [1]$\rangle$

- For $H \underset{subgroup}{\subseteq} G$: **The *quotient set* G/H** (of left side classes) $\stackrel{def}{=}$
  $G/H = \{gH \mid g \in G\}$.
  I.e. the *set* of *side classes* modulo H. $\langle$(4.1) p. 79 $\in$ [1]$\rangle$
  A.k.a. the *quotient* of G w.r.t. the *equivalence relation*. $\langle$obs. (4.4) p. 80 $\in$ [1]$\rangle$

- For $H \underset{subgroup}{\subseteq} G$: **The *quotient set* $H\backslash G$** (of right side classes) $\stackrel{def}{=}$
  $H\backslash G = \{Hg \mid g \in G\}$. $\langle$obs. (4.13) p. 83-84 $\in$ [1]$\rangle$

- $|G/H| = |G : H|$. $\langle$(4.1) p. 79 $\in$ [1]$\rangle$

- **The *canonical map*** $\stackrel{def}{=} g \mapsto gH : G \to G/H$.
  Maps an *element* of G to its *equivalence class*. $\langle$(4.4) p. 80 $\in$ [1]$\rangle$

- For groups: G, H, K where $H, K \underset{subgroup}{\subseteq} G$:
  $H \cap K$ *subgroup* but $H \cdot K$ *not* subgroup.
  $H \cdot K$ is a *union* of *side classes* modulo H and:
  $|H \cdot K| = |H : H \cap K| \cdot |K|$.
  For $K \subseteq H$ we have: $|G : K| = |G : H| \cdot |H : K|$. $\langle$lemma (4.11) p. 82 $\in$ [1]$\rangle$

- N **is a *normal* subgroup of** $G \overset{def}{=}$
  N is a *subgroup* of G and $\forall g \in G : gN = Ng$. ⟨(4.13) p. 84 ∈ [1]⟩

- For $N \underset{normal\ subgroup}{\subseteq} G$:
  There exists *precisely one composition* in G/N such that:
  $\forall g_1, g_2 \in G : (g_1 N) * (g_2 N) = g_1 g_2 N$.
  $(G/N, *)$ is a *group* with neural element $N = eN$. ⟨(4.13) p. 84 ∈ [1]⟩
  $(G/N, *)$ is called **the *quotient group***. ⟨def. (4.15) p. 85 ∈ [1]⟩
  Additively written: $(g_1 + N) + (g_2 + N) = (g_1 + g_2) + N$.

- The following are equivalent: ⟨(4.13) p. 84 ∈ [1]⟩
  1. $\forall g \in G : gN = Ng$. (i.e. N is *normal*)
  2. $\forall g \in G : gNg^{-1} = N$
  3. $\forall g \in G : gNg^{-1} \subseteq N$

- If $H \underset{subgroup}{\subseteq} G$ and $|G : H| = 2$, then:
  H is *normal*. ⟨obs. (4.17) p. 86 ∈ [1]⟩

- The *trivial subgroups* $\{e\}$ and G of G are *always normal*. ⟨(4.16) p. 85 ∈ [1]⟩

- G *commutative* $\Rightarrow$
  any subgroup $N \subseteq G$ is *normal* and G/N is *normal*. ⟨(4.17) p. 85 ∈ [1]⟩

2.9 Homomorphism and Isomorphism

Premises: G, G' ***groups***.

- **A *group homomorphism* (a.k.a. *homomorphism*)** $\phi : G \to G' \overset{def}{=}$ $\forall x, y \in G : \phi(xy) = \phi(x)\phi(y)$. ⟨(5.1.1) p. 89 ∈ [1]⟩
  Here we use *multiplicative notation* for elements of *both groups*.
- **A *group isomorphism* (a.k.a. *isomorphism*)** $\phi : G \to G' \overset{def}{=}$ ϕ is a *group homomorphism* and is *bijective*. ⟨(5.1.1) p. 89 ∈ [1]⟩
- For *homomorphism* $\phi : G \to G'$: ⟨(5.3) p. 89 ∈ [1]⟩
  - If $H \underset{subgroup}{\subseteq} G$, then $\phi(H)$ is a *subgroup* of G'.
  - If $H' \underset{subgroup}{\subseteq} G'$, then $\phi^{-1}(H')$ is a *subgroup* of G.
- **The *kernel* of a *homomorphism*** $\phi : G \to G' \overset{def}{=} \phi^{-1}(\{e\})$.
  I.e. the *preimage* of the *neutral element*. ⟨(5.3) p. 89 ∈ [1]⟩
  - We have: $\phi^{-1}(\{e\}) \underset{normal\ subgroup}{\subseteq} G'$. ⟨lemma (5.4) p. 90 ∈ [1]⟩
- **The *image* of G for a *homomorphism*** $\phi : G \to G' \overset{def}{=} \phi(G)$.
  ⟨(5.3) p. 89 ∈ [1]⟩
  - We have: $\phi(G) \underset{subgroup}{\subseteq} G'$. ⟨(5.3) p. 89 ∈ [1]⟩
- For *homomorphism* $\phi : G \to G'$:
  - $\phi(e) = e'$. ⟨obs (5.2) p. 89 ∈ [1]⟩
  - $\phi(x^{-1}) = (\phi(x))^{-1}$. ⟨obs (5.2) p. 89 ∈ [1]⟩
  - ϕ *injective* $\Leftrightarrow \phi^{-1}(\{e'\}) = \{e\}$. ⟨lemma (5.4) p. 90 ∈ [1]⟩
- *Composition* of 2 *homomorphisms* $\phi \circ \psi$ forms a new *homomorphism*.
- General examples of *homomorphisms*:
  - The ***trivial homomorphism*** $\phi : G \to G'$: $\forall g \in G : \phi(g) = e'$.
    Kernel: $\phi^{-1}(\{e'\}) = G$. *Image*: $\phi(G) = \{e\}$. ⟨ex (5.5) p. 90 ∈ [1]⟩
  - The ***inclusion map*** $\phi : H \to G$ for $H \underset{subgroup}{\subseteq} G$: $\forall x \in H : \phi(x) = x$.
    Kernel: $\phi^{-1}(\{e'\}) = \{e\}$. *Image*: $\phi(H) = H$. ⟨ex (5.5)(1) p. 90 ∈ [1]⟩
    Injective homomorphism. E.g. $x \mapsto x : \mathbb{R} \to \mathbb{C}$.
  - The ***canonical map*** $\phi : G \to G/N$ for $N \underset{normal\ s.gr.}{\subseteq} G$: $\phi(x) = xN$.
    Kernel: $\phi^{-1}(\{e'\}) = N$. *Image*: $\phi(G) = G/N$. ⟨ex (5.5)(2) p. 90 ∈ [1]⟩
    Sujective homomorphism. Rule: $g_1N \cdot g_2N = g_1g_2N$.
  - $\phi = i \mapsto g^i : \mathbb{Z} \to G$ for some $g \in G$. Rule: $g^{i+j} = g^i g^j$.
    Kernel: $\phi^{-1}(\{e'\}) = \mathbb{Z}n$, where $n = |g|$ (if ϕ is *not injective*).
    The kernel is $\{0\}$ if ϕ is *injective*, i.e. if $|g| = \infty$.
    Image: $\phi(\mathbb{Z}) = \langle g \rangle$, i.e. the *cyclic subgroup* produced by g.
    ⟨ex (5.5)(3) p. 90 ∈ [1]⟩

- Very concrete examples of *homomorphisms*:
  - $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$. Rule: $e^{x+y} = e^x e^y$.
    Kernel: $\exp^{-1}(\{1\}) = \{0\}$. *Image*: $\exp(\mathbb{R}) = \mathbb{R}^*_+$. ⟨ex (5.5)(5) p. 90 ∈ [1]⟩
    Injective, so it is an *isomorphism* when considered as map into $\mathbb{R}^*_+$.
  - $\log : (\mathbb{R}^*, \cdot) \to (\mathbb{R}, +)$. Rule: $\log(xy) = \log x + \log y$.
    Kernel: $\log^{-1}(\{0\}) = \{1\}$. *Image*: $\log(\mathbb{R}^*_+) = \mathbb{R}$. ⟨ex (5.5)(5) p. 90 ∈ [1]⟩
    Bijective when considered a map from $\mathbb{R}^*_+$, inverse of exp.
  - $\exp : (\mathbb{C}, +) \to (\mathbb{C}^*, \cdot)$.
    Kernel: $\exp^{-1}(\{1\}) = 2\pi i\mathbb{Z}$. *Image*: $\exp(\mathbb{C}) = \mathbb{C}^*$. ⟨ex (5.5)(5) p. 91 ∈ [1]⟩
  - $\phi = \theta \mapsto e^{i\theta} : \mathbb{R} \to \mathbb{U}$. *Surjective.* ⟨ex (5.5)(5) p. 91 ∈ [1]⟩
    Kernel: $\phi^{-1}(\{1\}) = 2\pi\mathbb{Z}$. *Image*: $\phi(\mathbb{R}) = \mathbb{U}$.
  - $sign : S_n \to \{\pm 1\}$. *Surjective* for $n > 1$. ⟨ex. (5.5) (4) p. 90 ∈ [1]⟩
    Kernel: A_n. *Image*: $\{\pm 1\}$ for $n > 1$ and $\{1\}$ for $n = 1$.
  - $\det : GL_n(\mathbb{R}) \to (\mathbb{R}^*, \cdot)$. Rule: $\det(AB) = \det(A)\det(B)$.
    Kernel: $SL_n(\mathbb{R})$. *Image*: $\mathbb{R}^*$.
    So, $SL_n(\mathbb{R})$ is *normal* in $GL_n(\mathbb{R})$. ⟨ex. (5.6) (4) p. 91 ∈ [1]⟩
  - $\det : O_n(\mathbb{R}) \to (\{\pm 1\}, \cdot)$.
    Kernel: $SO_n(\mathbb{R})$. *Image*: $\{\pm 1\}$. So, $SO_n(\mathbb{R})$ is *normal* in $O_n(\mathbb{R})$.
- *Homomorphism theorem*:
  Let $\kappa : G \to \bar{G}$ be a *surjective homomorphism* with *kernel* N.
  Let $\phi : G \to G'$ be *any homomorphism* with $\phi(N) = \{e'\}$.
  Then there *exists exactly one* $\bar{\phi} : \bar{G} \to G'$ such that
  $\forall g \in G : \bar{\phi}(\kappa(g)) = \phi(g)$. ⟨thm. (5.6) p. 91 ∈ [1]⟩
- Notice: We say that ϕ *vanishes on* N when $\phi(N) = \{e'\}$. ⟨obs. (5.7) p. 92 ∈ [1]⟩
- Standard application of homomorphism theorem is on
  the *canonical homomorphism* $g \mapsto gN : G \to G/N$
  for some *normal subgroup* N of G.
  The homomorphism $\bar{\phi} : G/N \to G$ is said to be *induced* by ϕ.
  I.e.: If $\phi(N) = \{e'\}$ then $\exists!\bar{\phi}$ *homomorphism* such that $\bar{\phi}(gN) = \phi(g)$.
  ⟨obs. (5.7) p. 92 ∈ [1]⟩
- *Isomorphism theorem*:
  Let $\phi : G \to G'$ be a *homomorphism* with *kernel* $N = \phi^{-1}(\{e'\})$.
  For $\kappa : g \mapsto gN : G \to G/N$, the *induced homomorphism* $\bar{\phi}([g]) = \phi(g)$ is an *isomorphism* $G/\phi^{-1}(\{e'\}) \xrightarrow{\sim} \phi(G)$ of the *quotient* of G *modulo* the *kernel* on the *image group* $\phi(G)$. ⟨thm. (5.8) p. 92 ∈ [1]⟩
- Examples of *isomorphisms* and use of *isomorphism theorem*:
  - For some $g \in G$ we have: $i \mapsto g^i : \mathbb{Z} \to G$ is a *homomorphism.*
    For $|g| = \infty$, it is an *isomorphism.*
    For $|g| = n$, the *kernel* is $\mathbb{Z}n$. From the *isomorphism theorem,*
    we can *induce* an *isomorphism* $\mathbb{Z}/\mathbb{Z}n \xrightarrow{\sim} \langle g \rangle$. ⟨ex. (5.9)(1) p. 92 ∈ [1]⟩
  - $sign : S_n \to \{\pm 1\} = C_2$ is a *homomorphism* with *kernel* A_n.
    For $n \geq 2$ it is *surjective* and *induces an isomorphism* $S_n/A_n \xrightarrow{\sim} C_2$.
    ⟨ex. (5.9)(2) p. 92 ∈ [1]⟩

- $\exp : \mathbb{C} \to \mathbb{C}^*$ is a *surjective homomorphism* with *kernel* $2\pi i\mathbb{Z}$.
  It *induces* an *isomorphism* $\mathbb{C}/2\pi i\mathbb{Z} \overset{\sim}{\to} \mathbb{C}^*$. ⟨ex. (5.9)(3) p. 92 ∈ [1]⟩
  Similarly, $t \mapsto e^{it}$ *induces* an *isomorphism* $\mathbb{R}/2\pi\mathbb{Z} \overset{\sim}{\to} \mathbb{U}$.
- *det* : $GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a *surjective homomorphism* with *kernel* $SL_n(\mathbb{R})$.
  It *induces* an *isomorphism* $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \overset{\sim}{\to} \mathbb{C}^*$. ⟨ex. (5.9)(4) p. 92 ∈ [1]⟩

- For *isomorphism* $\phi : \phi^{-1}(\{e'\}) = \{e\}$.
- **Two groups G, G' are *isomorphic*** $\overset{def}{=}$
  there *exists* an *isomorphism between them.* ⟨def. (5.10) p. 93 ∈ [1]⟩
- For $\phi : G \to G'$ *isomorphism*, $\phi^{-1} : G' \to G$ is *also an isomorphism.*
  ⟨def. (5.10) p. 93 ∈ [1]⟩
- *Isomorphic groups* have the *same group structure* ⟨def. (5.10) p. 93 ∈ [1]⟩
  (i.e. the same composition table except for element names).
  All derived group properties are therefore the same for isomophic groups, e.g. there is *only one cyclic group* C_n of *order* n, except for isomorphism.
- *Noether's First Isomorphism Theorem*: ⟨thm (5.13) p. 94 ∈ [1]⟩
  Let H, N be *subgroups* of G, where N is *normal.* Then:
  - $HN = \{hn \mid h \in H \land n \in N\}$ is a *subgroup* of G.
  - N is a *normal subgroup* of HN.
  - $H \cap N$ is a *normal subgroup* of H.
  - There exists a natural *isomorphism*: $H/(H \cap N) \overset{\sim}{\to} HN/N$.

  This further implies: ⟨obs (5.14) p. 94 ∈ [1]⟩
  - $|H : H \cap N| = |HN : N|$.
  - $|HN| = |HN : N| \cdot |N|$ (from the *Index Theorem*).
  - $|HN| = |H : H \cap N| \cdot |N|$.
- *Noether's Second Isomorphism Theorem*: ⟨thm (5.15) p. 94-95 ∈ [1]⟩
  Let $\phi : G \to G'$ be a *homomorphism* with *kernel* $K = \phi^{-1}(\{e'\})$. Then:
  - $H \mapsto \phi(H)$ is a *bijective map* from the
    set of *subgroups* of G which include K to the set of *subgroups* of $\phi(G)$.
    Its *inverse* is $L \mapsto \phi^{-1}(L)$ for *subgroups* L of $\phi(G)$.
  - For a *subgroup* N of G with $N \supseteq K$:
    N *normal* in $G \Leftrightarrow \phi(N)$ *normal* in $\phi(G)$.
  - For a *normal subgroup* N of G with $N \supseteq K$:
    There exists a natural *isomorphism*: $G/N \overset{\sim}{\to} \phi(G)/\phi(N)$.
- Noether's Second Iso. Thm. is often used on the canonical (surjective) homomorphism $G \to G/K$ where K is a given *normal* subgroup of G.
  For $H \underset{subgroup}{\subseteq} G$ where $H \supseteq K$, the *image* consists of the sideclasses hK, for $h \in H$. So the image can be identified with the quotient group H/K.
  The theorem claims that all subgroups in G/K has the form H/K for a uniquely determined subgroup $H \supseteq K$.
  Furthermore, the *normal* subgroups of G/K are the subgroups N/K, where $N \supseteq K$ is *normal* in G.
  The *isomorphism* here is: $G/H \overset{\sim}{\to} (G/K)/(N/K)$. ⟨obs (5.17) p. 96 ∈ [1]⟩

2.10 Structure Theorem for Commutative Groups

- **The *product* of r groups** $G_1, \ldots, G_r \overset{def}{=} G_1 \times \cdots \times G_r$ with *coordinatewise composition*: $(g_1, \ldots, g_r)(b_1, \ldots, b_r) \mapsto (g_1 h_1, \ldots, g_r h_r)$.
  $G_1 \times \cdots \times G_r$ is also called the ***direct product*** of $G_1, \ldots, G_r$.
  For *additively written groups*: The *direct sum*: $G_1 \oplus \cdots \oplus G_r$.
  ⟨(6.1) p. 99 ∈ [1]⟩

- $|G_1 \times \cdots \times G_r| = |G_1| \cdots |G_r|$. ⟨(6.1) p. 99 ∈ [1]⟩

- The i'th *projection*: $(g_1, \ldots, g_r) \mapsto g_i$ is a *surjective homomorphism*.
  ⟨(6.1) p. 99 ∈ [1]⟩

- The i'th *injection*: $g_i \mapsto (e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_r)$ for $g_i \in G_i$.
  ⟨(6.1) p. 99 ∈ [1]⟩

- **G is the *direct product* of the subgroups** $H_1, \ldots, H_r \overset{def}{=}$ there exists a *homomorphism* $H_1 \times \cdots \times H_r \to G$.
  Also written: $H_1 \times \cdots \times H_r = G$. ⟨(6.1) p. 99 ∈ [1]⟩

- Let $n = n_1 \cdots n_r$ be a *product* of *primic natural numbers* n_i.
  The Chinese Remainder Class Theorem says that:
  $\phi = [x]_n \mapsto ([x]_{n_1}, \ldots, [x]_{n_r}) : \mathbb{Z}/n \underset{\to}{\sim} \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ is *bijective*.
  It is also an *isomorphism*.
  So $\mathbb{Z}/n$ is *isomorphic* to the direct product $\mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$.
  Since x is *primic* to n if and only if x is primic to *each factor* n_i,
  ϕ also defines an *isomorphism* $(\mathbb{Z}/n)^* \underset{\to}{\sim} (\mathbb{Z}/n_1)^* \times \cdots \times (\mathbb{Z}/n_r)^*$.
  ⟨(6.3) p. 100 ∈ [1]⟩

- For *subgroups* $H_1, \ldots, H_r$ of G, consider the map
  $\phi = (h_1, \ldots, h_r) \mapsto h_1 \cdots h_r : H_1 \times \cdots \times H_r \to G$.
  ϕ is a *homomorphism* $\Leftrightarrow \forall i < j, h_i \in H_i, h_j \in H_j : h_i h_j = h_j h_i$.
  This is a *necessary condition* for G to be a *direct product* of $H_1, \ldots, H_r$.
  For G *commutative*, ϕ is thus *always* a *homomorphism*. ⟨(6.2) p. 100 ∈ [1]⟩

- Let G be a group and $H, K \underset{subgroups}{\subseteq} G$. Then the following are equivalent:

  1. G is the *direct product* of H and K, i.e.:
     $(h, k) \mapsto hk : H \times K \to G$ is an *isomorphism*.
  2. H, K are *normal* and $H \cap K = \{e\}$ and $HK = G$.

  ⟨lemma (6.4) p. 101 ∈ [1]⟩

- Let $n = n_1 \cdots n_r$ be a *product* of *pairwise primic* numbers n_i.
  Let G be a *commutative group* of *order* n.
  Then every subset $H_i = \{g \in G \mid g^{n_i} = e\}$ is a *subgroup* of G and
  G is the *direct product* of the subgroups H_i, i.e.: $H_1 \times \cdots \times H_r \overset{\sim}{\rightarrow} G$.
  ⟨thm (6.5) p. 101 ∈ [1]⟩
  Furthermore: $|H_i| = n_i$. ⟨obs (6.6) p. 102 ∈ [1]⟩

- The standard application of the above theorem is on the
  prime resolution $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$.
  For *commutative group* G with $|G| = n$,
  the p_i are the *prime divisors* in $|G|$.
  For such a p_i, H_i is the group of elements g with $g^{p_i^{\nu_i}} = e$.
  The *elements* have *order* $p_i^{\mu_i}$ with $0 \leq \mu_i \leq \nu_i$.
  These H_i are called $G(p_i)$. $|G(p_i)| = p_i^{\nu_i}$.
  From the theorem, G is the *direct product* of its subgroups $G(p_i)$.
  ⟨obs (6.6) p. 102 ∈ [1]⟩

- Let G be a *commutative group* and G_0 be a *subgroup* of G.
  Let $\phi : G \to \bar{G}$ be a *surjective homomorphism*.
  If $\phi|_{G_0} : G_0 \to \bar{G}$ is *bijective*, then
  G is the *direct product* of G_0 and the *kernel* for ϕ:
  $G_0 \times \phi^{-1}(\{\bar{e}\}) \overset{\sim}{\rightarrow} G$. ⟨lemma (6.7) p. 102 ∈ [1]⟩

- Let G be a *finite abelian* group and let
  m be the *maximal order* of the elements of G. ⟨thm (6.8) p. 103 ∈ [1]⟩
  Then *every element* in G has an *order* which is *divisor* in m.

- Let G be a *finite commutative* group and
  $g_0 \in G$ be an *element* with *maximal order* m.
  Then there exists a *subgroup* K of G such that
  G is the *direct product* of $\langle g_0 \rangle$ and K: $\langle g_0 \rangle \times K \overset{\sim}{\rightarrow} G$. ⟨thm (6.9) p. 103 ∈ [1]⟩

- *Structure Theorem for Abelian Groups*: ⟨(6.10) p. 104 ∈ [1]⟩
  The following holds for a *finite abelian group* G of *order* n:

  1. G is *isomorphic* to some *product* of *cyclic groups*:
     $G \simeq C_{m_1} \times \cdots \times C_{m_r}$, where $\forall i \in \{1, \ldots, r\} : m_i \geq 1$.
     Here, the *trivial group* is given by $r = 0$, (i.e. *no products*).
  2. The *orders* $m_1, \ldots, m_r$ can *chosen uniquely* by:
     $\forall i \in \{1, \ldots, r\} : m_{i+1} | m_i$ (i.e.: m_{i+1} divisor in m_i).
  3. Alternatively, the *orders* $m_1, \ldots, m_r$ can *chosen uniquely* such that:
     each m_j is a *prime power*.

  Note: The Chinese Remainder Class Theorem is a special case of this.

- From the above, there are as many *finite abelian* groups of a *given order*
  n, as there are ways to partition all *exponents* ν_i in the *prime resolution*:
  $n = p_1^{\nu_1} \cdots p_s^{\nu_s}$. ⟨obs (6.11) p. 106 ∈ [1]⟩

Examples of Finite Groups

- There are exactly 3 *commutative groups* of *order* $24 = 2^3 3$:
  $C_{24} = C_8 \times C_3, \qquad C_{12} \times C_2 = C_4 \times C_2 \times C_3,$
  $C_6 \times C_2 \times C_2 = C_2 \times C_2 \times C_2 \times C_3.$
  All the *possibilities* follow from the partitions of the prime powers.
  The *isomorphisms* follow from the theorem about primic products for n:
  $n = n_1 \cdots n_r$. ⟨ex (6.12) p. 106 ∈ [1]⟩

- Number of groups with order 16: Number of *partitions* into *prime powers*:
  C_{16}, $C_8 \times C_2$, $C_4 \times C_4$, $C_4 \times C_2 \times C_2$, $C_2 \times C_2 \times C_2 \times C_2$ gives
  all commutative groups.
  Non-commutative: D_8, $D_4 \times D_2$, $Q_8 \times C_2$, ... (many non-commutative).
  How to they differ: (e.g. it holds that $D_6 \simeq D_3 \times D_2$, so no difference).
  D_8 has an *element* of *order* 8.
  D_4 has element orders of only $1, 2, 4$. So $D_8 \neq D_4 \times D_2$.
  Q_8 has 6 elements of order 4. So $Q_8 \times C_2$ has 12.
  D_4 has only 2 elements of order 4. So $D_4 \times D_2$ has 8.

2.11 Group Effects ⟨ DK: Gruppevirkninger ⟩

- **An *outer composition*** (on X) $\overset{def}{=}$ a map $G \times X \to X$. ⟨(7.3) p. 110 ∈ [1]⟩
- The *effect point of view*:
  The group G where ($1 \in G$ is neutral) ***affects*** **X from the *left*** $\overset{def}{=}$
  There is a given map $(g, x) \mapsto g.x : G \times X \to X$ where:
  $g.(h.x) = (gh).x$ and $1.x = x$. ⟨def (7.2) p. 109 ∈ [1]⟩
  Alternative notations: $(g, x) \mapsto gx$ or $(g, x) \mapsto {}^g x$. ⟨(7.3) p. 110 ∈ [1]⟩
  Additive notation: $g.(h.x) = (g + h).x$ and $0.x = x$. ⟨(7.3) p. 110 ∈ [1]⟩
- **A *right-effect* of G on X** $\overset{def}{=}$ ⟨(7.3) p. 110 ∈ [1]⟩
  A composition $(g, x) \mapsto g.x$ where $x.1 = x$ and $x.(gh) = (x.g).h$.
- **X is a G set** $\overset{def}{=}$ G is a given *effect* on X. ⟨def (7.2) p. 109 ∈ [1]⟩
- For fixed g we get a *bijective* map $\rho_g = g_X = x \mapsto g.x$ where
  $(gh)_X = g_X \circ h_X$ (also written: $\rho_{gh} = \rho_g \circ \rho_h$) and $1_X = id_X$.
  Furthermore, $\rho_g \in Perm(X)$ and its *inverse* is: $(\rho_g)^{-1} = \rho_{g^{-1}}$.
- The *representation point of view*:
  The *representation* ρ of the *effect* of G on X $\overset{def}{=}$
  $\rho = g \mapsto \rho_g : G \to Perm(X)$.
  ρ is a *group homomorphism* because of $(gh)_X = g_X \circ h_X$. ⟨def (7.2) p. 109 ∈ [1]⟩
  Each $g \in G$ is *represented* by $\rho_g \in Perm(X)$.
  Conversely, given a *homomorphism* $\rho : G \to Perm(X)$,
  $g.x = \rho_g(x)$ defines an *effect* of G on X. ⟨def (7.2) p. 109 ∈ [1]⟩

Well-known Effects and Examples

- **The *trivial effect* of G on X** $\overset{def}{=}$ $\forall g \in G, x \in G : g.x = x$.
  Its *representation* is also the *trivial homomorphism* $G \to Perm(X)$.
  ⟨(7.4) p. 110 ∈ [1]⟩
- $G \underset{subgroup}{\subseteq} Perm(X)$ affects X by: $\forall \sigma \in G, x \in X : \sigma.x = \sigma(x)$.
  The corresponding *representation*
  is the *inclusion homomorphism* $G \to Perm(X)$. ⟨ex. (7.5)(1) p. 110 ∈ [1]⟩
- $GL_n(\mathbb{R})$ affects $\mathbb{R}^n$ by: $\forall g \in GL_n(\mathbb{R}), x \in \mathbb{R}^n : g.x = gx$.
  the gx here is the *matrix product* with x as a *column vector*.
  The corresponding *representation*
  maps the *matrix* g on to the *bijective map* $x \mapsto gx$. ⟨ex. (7.5)(2) p. 110 ∈ [1]⟩
- For *real vector space* V, *multiplication* of *vectors* with *scalars* different from 0 is an *effect* of the *multiplicative group* $\mathbb{R}^*$ on V. ⟨ex. (7.5)(3) p. 110 ∈ [1]⟩
- **G *affects itself* by *translation*** by $\overset{def}{=}$ $\forall g.x \in G : g.x = gx$.
  By $x.g = xg$ we define a *right-effect* of G on itself. ⟨(7.6) p. 111 ∈ [1]⟩
- *Cayley's theorem*: Let G be a *group* which *affects itself* by *translation*.
  Then the corresponding *representation* is an *injective homomorphism*
  $\rho : G \to Perm(G)$. ⟨thm (7.7) p. 111 ∈ [1]⟩

- Let G affect X and $H \underset{subgroup}{\subseteq} G$.
  A subset $Y \subseteq X$ is H-*stable* (a.k.a. H-*invariant*) $\stackrel{def}{=}$ $y \in Y, h \in H \Rightarrow h.y \in Y$. ⟨(7.8) p. 111 ∈ [1]⟩

- Let G affect X, $H \underset{subgroup}{\subseteq} G$, $Z \subseteq X$ and Z be H-*invariant*, then:
  H affects Z by $(h, z) \mapsto h.z : H \times Z \to Z$.
  It is said to be defined by ***restriction* of the given effect of G on X.** ⟨(7.8) p. 111 ∈ [1]⟩

- By *restriction* of the effect of G on X,
  an effect of $H \underset{subgroup}{\subseteq} G$ on X is always defined. ⟨(7.8) p. 111 ∈ [1]⟩

- Any G-*invariant* subset $Z \subseteq X$ defines an effect of G on Z. ⟨(7.8) p. 111 ∈ [1]⟩

- Let G affect X (from the *left*), then the following holds:

  1. G affects the *power set* $\mathcal{P}(X)$, where for each $A \subseteq X$ we define:
     $g.A = \{g.a \mid a \in A\}$. ⟨(7.8) p. 111 ∈ [1]⟩
  2. G affects the *product set* $X \times X$ by:
     $g.(x_1, x_2) = (g.x_1, g.x_2)$. ⟨(7.8) p. 111 ∈ [1]⟩
  3. For *arbitrary set* Y, G affects $X^Y = \{\phi : Y \to X\}$ by:
     $(g.\phi)(y) = g.(\phi(y))$. (Curry's theorem says: $(X^Y)^Z = X^{Y \times Z}$).
     $g.\phi = g_X \circ \phi$, for $\phi : Y \to X$.
     Warning: $Y^X = \{\psi : X \to Y\}$ does *not* hold for $g.\psi(x) = \psi(g.x)$, which means that the group *affects* from the *right*. ⟨(7.8) p. 111 ∈ [1]⟩
  4. For *arbitrary set* Y, G affects $Y^X = \{\eta : X \to Y\}$ by:
     $(g.\eta)(x) = \eta(g^{-1}.x)$. ⟨(7.8) p. 111 ∈ [1]⟩

- $\mathbb{R}$ affects itself by *translation*: For $t \in \mathbb{R} : \rho_t(x) = x + t$.
  $\mathbb{R}$ affects all maps $\eta : \mathbb{R} \to Y$ for arbitrary Y by:
  $(\rho_t.\eta)(x) = \eta(\rho_t^{-1}.x) = \eta(x - t)$. ⟨ex. (7.9) p. 112 ∈ [1]⟩

- D_n affects $\mathbb{R}^2$ by *restriction* of $GL_n(\mathbb{R})$ to its *subgroup* D_n.
  Let $X = \{p_1, p_2, \ldots, p_n = p_0\}$ be the n *invariant corners* of D_n.
  D_n affects the n *corners* X with the *representation*
  $\rho : D_n \to S_X$, which is a *homomorphism.*
  ρ is *injective* for $n \geq 3$. ⟨ex. (7.10) p. 112 ∈ [1]⟩

- The *hexaeder group H affects* the following: ⟨ex. (7.11) p. 112 ∈ [1]⟩

  1. The set of 8 *corners*, with *representation* $H \to S_8$.
  2. The set of 6 *face mid-points*, with *representation* $H \to S_6$.
  3. The system of 12 *edges*, with *representation* $H \to S_{12}$.
  4. The system of 6 *faces*, with *representation* $H \to S_6$
     (identical to 6 facepoints).
  5. The system of 4 *corner axes*, with *representation* $H \to S_4$
     $H \to S_4$ is *bijective* and H is *isomorphic* to S_4.
  6. The system of 3 *face axes*, with *representation* $H \to S_3$
     $H \to S_3$ is *surjective* with *kernel* V (Klein's Vier group).

G-equivalence, Orbits, Fixpoints, Isotropy

Premises: G ***affects*** X.

- $x, x' \in X$ **are** G**-*equivalent*:** $x \underset{G}{\sim} x'$ (or just: $x \sim x'$) $\overset{def}{=}$ $\exists g \in G : x' = g.x$. $\underset{G}{\sim}$ is an *equivalence relation.* ⟨(7.12) p. 112 ∈ [1]⟩
- **The *orbit* ⟨ DK: banen ⟩ $G.x$ of G through $x \in X$** $\overset{def}{=}$ the *equivalence class* w.r.t. $\underset{G}{\sim}$ *containing* $x \in X$: $G.x = \{g.x \mid g \in G\}$. ⟨(7.12) p. 113 ∈ [1]⟩
- **The *orbit length* ⟨ DK: banelængden ⟩** $|G.x|$ $\overset{def}{=}$ $|G.x|$ is the *number of elements* in $G.x$. ⟨(7.12) p. 113 ∈ [1]⟩
- **The *orbit space* ⟨ DK: banerummet ⟩** X/G $\overset{def}{=}$ X/G is the *set of equivalence classes* w.r.t. $\underset{G}{\sim}$,
  i.e.: the *quotient* of X w.r.t. G*-equivalence.* ⟨(7.12) p. 113 ∈ [1]⟩
  Its *elements* are subsets of X of the form $G.x$ with $x \in X$.
  It would be natural to use the notation $G\backslash X$ (still read: "X modulo G").
  Note: Don't confuse with set complement. ⟨rem. (7.14) p. 114 ∈ [1]⟩
- $x \in X$ **is *fixpoint* for** $g \in G$ $\overset{def}{=}$ $g.x = x$. ⟨(7.12) p. 113 ∈ [1]⟩
  Also said: x **is *invariant* under** G or g ***stabilizes*** x.
- **The *set of fixpoints*** X^g **for** $g \in G$ $\overset{def}{=}$ $X^g = \{x \in X \mid g.x = x\} \subseteq X$. ⟨(7.12) p. 113 ∈ [1]⟩
- $x \in X$ **is *fixpoint* for the *effect*** G (a.k.a. x **is** G**-*invariant***) $\overset{def}{=}$ $\forall g \in G : x = g.x$. ⟨(7.12) p. 113 ∈ [1]⟩
- **The *set of fixpoints*** X^G **for the *effect*** G $\overset{def}{=}$ $X^G = \bigcap_{g \in G} X^g = \{x \in X \mid \forall g \in G : g.x = x\} =$ $\{x \in X \mid G_x = G\} = \{x \in X \mid G.x = \{x\}\}$. ⟨(7.12) p. 113 ∈ [1]⟩
- **The *isotropy group*** G_x **for** $x \in X$
  (a.k.a. the ***stabilizor group* for** x) $\overset{def}{=}$
  $G_x = \{g \in G \mid g.x = x\} \subseteq G$.
- $x \in X$ is a *fixpoint* for the *effect* $G \Leftrightarrow G_x = G$. ⟨(7.12) p. 113 ∈ [1]⟩
- $x \in X$ is a *fixpoint* for the *effect* $G \Leftrightarrow G.x = \{x\}$. ⟨(7.12) p. 113 ∈ [1]⟩
- The *orbit formula*: ⟨rem. (7.15) p. 114-115 ∈ [1]⟩
  For $x \in X$ the map $g \mapsto g.x : G \to X$ is *constant* on
  each *side class modulo* the *isotropy group* G_x.
  It *induces* a *bijective* map $G/G_x \overset{\sim}{\to} G.x$ of
  the left side classes modulo the isotropy group G_x on the orbit $G.x$.
  Orbit length: $|G.x| = |G : G_x|$.
  I.e. the orbit length equals the *index* of the *isotropy group* G_x.
  For *finite* G: The *orbit length* is *divisor* in $|G|$.

Examples

Premises: G ***affects*** X.

Effect and Misc Description	Orbits	Fixpoints	Ref.
Trivial effect of G on X *G-equivalence* is just *equality*	all *one-point* sets	*all points* are fixpoints for the *effect*	⟨(7.13)(1) p. 113 ∈ [1]⟩
Effect of $G = Perm(X)$ on *finite* X. *All elements* are *equivalent*	*one orbit* consisting of *all points*		⟨(7.13)(2) p. 113 ∈ [1]⟩
Effect of $G = \langle\sigma\rangle$ on *finite* X, for $\sigma \in Perm(X)$	the *orbits* of the *permutation* σ	the *fixpoints* $x \in X$ of the *permutation* σ	⟨(7.13)(2) p. 113 ∈ [1]⟩
Effect of $GL_n(\mathbb{R})$ on $\mathbb{R}^n$	$\{\vec{0}\}$ and $\mathbb{R}^n \backslash \{\vec{0}\}$	*eigenvectors* $x \in X$ with *eigenvalue* 1 of the *linear* map $x \mapsto gx$. $\vec{0}$ is fixpoint for the *effect*	⟨(7.13)(3) p. 114 ∈ [1]⟩
Effect of $\mathbb{R}^*$ on a *vector space* V by *multiplication* of *vectors* with *scalars*	$\{\vec{0}\}$ and all 1-*dim. subspaces* (lines) *excluding* $\vec{0}$	$\vec{0}$ is fixpoint for the *effect*	⟨(7.13)(4) p. 114 ∈ [1]⟩
Effect of *additive* $\mathbb{R}$ on $\mathbb{C}$ by *rotations.* Representation: $\rho_t(z) = e^{it}z$	$(0,0)$ and all *circles* with *center* $(0,0)$	$(0,0)$ is fixpoint for *effect*	⟨(7.13)(5) p. 114 ∈ [1]⟩
Effect of G on $X = G$ by *translation.* *All elements* are *G-equivalent.* For any $x \in G : G_x = \{1\}$	*one orbit* consisting of *all points*		⟨(7.13)(6) p. 114 ∈ [1]⟩
Effect of *restriction* of G to H on G by *translation*	The *right side classes* Hx. *Orbit space*: $H\backslash G$		⟨(7.13)(6) p. 114 ∈ [1]⟩
Effect of *additive* $\mathbb{R}$ on *functions* $\eta : \mathbb{R} \to Y$. For given $t \in \mathbb{R}$: $\rho_t\eta(x) = \eta(x - t)$.		η is fixpoint for t if η is *periodic* with period t	⟨(7.13)(7) p. 114 ∈ [1]⟩

(GRP7 p. 109-122 is missing)

2.12 Sylow's Theorems

- ***Sylow-p-subgroup* of** $G \overset{def}{=}$
  a *subgroup* S of *order* p^ν, where p is a *prime divisor* in $|G|$ and $|G| = n_0 p^\nu$ where $p \nmid n_0$. ⟨def. (8.2) p. 125 ∈ [1]⟩

- Any *conjugated subgroup* gHg^{-1} of a *Sylow-p-subgroup* H of G is *also* a *Sylow-p-subgroup* of G. ⟨def. (8.2) p. 125 ∈ [1]⟩

- For a *commutative* group G of *order* n where
  $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ is the *prime resolution* of n:
  G is the *direct product* of $G(p_i)$, where
  $G(p_i)$ is the subgroup of *elements* g of *orders* which are a *power* of p_i.
  The $G(p_i)$ have $|G(p_i)| = p_i^{\nu_i}$ and are *all* the *Sylow-p-subgroups* of G.
  ⟨ex. (8.3) p. 125 ∈ [1]⟩

- Examples:
  - D_7 (order: $14 = 7 \cdot 2$) has 1 *Sylow-7-subgroup* and 7 *Sylow-2-subgroups*. ⟨ex. (8.4) p. 125 ∈ [1]⟩
  - D_6 (order: $12 = 2^2 3$) has 1 *Sylow-3-subgroup* and 3 *Sylow-2-subgroups* (of order $2^2 = 4$). ⟨ex. (8.4) p. 125-126 ∈ [1]⟩
  - S_4 (order: $24 = 2^3 3$) has *Sylow-2-subgroup* and *Sylow-3-subgroups* (of orders 8 and 3). D_4 is a *Sylow-2-subgroup*. ⟨ex. (8.5) p. 126 ∈ [1]⟩
  - For A_5 (order: $60 = 2^2 3 \cdot 5$).
    The *subgroup* of *id* and the 3 *double transpositions* of 4 of the numbers $1, 2, 3, 4, 5$ is the *only Sylow-2-subgroup* (order 4).
    The *subgroups* produced by 3-*cycles* are *all Sylow-3-subgroups* (order 3).
    The *subgroup* produced by the 5-*cycle* is the *only Sylow-5-subgroups* (order 5). ⟨ex. (8.5) p. 126 ∈ [1]⟩

- For $n_0 \in \mathbb{N}$ and p *prime*: $\begin{pmatrix} n_0 p^\nu \\ p^\nu \end{pmatrix} \equiv n_0 \pmod{p}$. ⟨lemma (8.6) p. 126 ∈ [1]⟩

- The following holds when p is a *prime divisor* in the *order* $|G|$:
  1. There *exists Sylow-p-subgroups* of G.
  2. The *Sylow-p-subgroups* are *mutually conjugated* and any *p-subgroup* of G is *contained* in a *Sylow-p-subgroup*.
  3. The *number* of *Sylow-p-subgroups* is *congruent* with 1 modulo p and is *divisor* in $|G|$.

  ⟨Sylow's Theorems (8.7) p. 127 ∈ [1]⟩

- Let $|G| = n_0 p^\nu$ where p *prime* and $p \nmid n_0$.
  The *number* d of *Sylow-p-subgroups* is to be found among the numbers where $d | n_0$ and $d \equiv 1 \pmod{p}$. ⟨obs. (8.8) p. 128 ∈ [1]⟩

- The following are *equivalent*: ⟨obs. (8.8) p. 128 ∈ [1]⟩
  1. There is *exactly one Sylow-p-subgroup* of G.
  2. There *exists* a *normal Sylow-p-subgroup* in G.

- For G *commutative*:
  All subgroups are *normal* so for *each prime divisor* p_i in $|G|$
  there exists *exactly one Sylow-p_i-subgroup* of G. ⟨obs. (8.8) p. 129 ∈ [1]⟩

- For *prime divisor* p in $|G| = n_0 p^\nu$, where $p \nmid n_0$:
  A *subgroup* H of G has $|H|$ as *divisor* in $|G|$ and
  $|H| = m_0 p^\mu$, where $m_0 | n_0$ and $\mu \leq \nu$. ⟨obs. (8.9) p. 129 ∈ [1]⟩
  Furthermore:

  1. A *Sylow-p-subgroup* S of H has *order* p^μ and
     S is *only* a *Sylow-p-subgroup* of G if $\mu = \nu$. ⟨obs. (8.9) p. 129 ∈ [1]⟩
  2. $\mu = \nu \Leftrightarrow |G : H|$ is *primic* with p. ⟨obs. (8.9) p. 129 ∈ [1]⟩
  3. Assume $|G : H|$ is *primic* with p,
     so that *any Sylow-p-subgroup* of H is a *Sylow-p-subgroup* of G.
     If H is also *normal* in G, then the opposite also hold:
     Any *Sylow-p-subgroup* of G is *contained* in H. ⟨obs. (8.9) p. 129 ∈ [1]⟩
  4. When H is *normal* in G then:
     H has a *normal Sylow-p-subgroup* $\Leftrightarrow$
     G has a *normal Sylow-p-subgroup.* ⟨obs. (8.9) p. 129 ∈ [1]⟩

- For a group G of *order* n, with *prime resolution* $p_1^{\nu_1} \cdots p_r^{\nu_r} = n$ of n:
  If $(\forall i \in \{1, \ldots, r\} : G$ has a *normal Sylow-p_i-subgroup* $S_i)$ then
  G equals the *product* of its *Sylow-p_i-subgroups*: $S_1 \times \cdots \times S_r = G$.
  ⟨thm. (8.10) p. 129 ∈ [1]⟩

- There is *only one* group of *order* qp, where $q < p$ are 2 *prime numbers*
  and $p \neq 1 \pmod{q}$. This group is the *cyclic* C_{qp}. ⟨cor. (8.11) p. 130 ∈ [1]⟩
  Furthermore:

  1. $p \neq 1 \pmod{q}$ can *never* hold for $q = 2$. ⟨rem. (8.12) p. 130 ∈ [1]⟩
  2. For uneven *prime* p:
     There are *exactly* 2 groups of *order* $2p$: C_{2p} and D_p.
     ⟨rem. (8.12) p. 130 ∈ [1]⟩

- **The group G is *simple*** $\stackrel{def}{=}$ ⟨def. (8.13) p. 130 ∈ [1]⟩
  G is *not* the *trivial group* and
  the *trivial subgroups* $\{e\}$ and G are the *only normal subgroups* of G.

- *All simple groups* can be *classified.* ⟨def. (8.13) p. 130 ∈ [1]⟩

- The *only simple groups* of *uneven order* are C_p for p *prime number.*
  ⟨def. (8.13) p. 130 ∈ [1]⟩

- All the *simple commutative groups* are C_p for p *prime number.*
  ⟨def. (8.13) p. 130 ∈ [1]⟩

- The *alternating groups* A_n are *simple* for $n \geq 5$. ⟨thm. (8.17) p. 131 ∈ [1]⟩

- Examples:
  - S_n for $n \geq 3$ are *not simple.* (A_n *normal non-trivial* subgroups). ⟨ex. (8.15) p. 131 ∈ [1]⟩
  - D_n for $n \geq 2$ are *not simple.* (C_n *normal non-trivial* subgroups). ⟨ex. (8.15) p. 131 ∈ [1]⟩
  - A group of *order* $n_0 p^\nu$ for p *prime* and $1 < n_0 < p$, $\nu \geq 1$ *cannot* be *simple.* ⟨ex. (8.16) p. 131 ∈ [1]⟩
  - A group of *order* $2 \cdot 3$ has a *normal Sylow-3-subgroup.* ⟨ex. (8.16) p. 131 ∈ [1]⟩
  - A group of *order* $2 \cdot 5$, $3 \cdot 5$ or $4 \cdot 5$ has a *normal Sylow-5-subgroup.* ⟨ex. (8.16) p. 131 ∈ [1]⟩
  - A group of *order* $12 = 2^2 \cdot 3$ *either* has a *normal Sylow-2-subgroup* *or* has a *normal Sylow-3-subgroup.* ⟨ex. (8.16) p. 131 ∈ [1]⟩

3 Rings and Fields ⟨ DK: Legemer ⟩

- **A *ring*** $(\Lambda, +, \cdot) \overset{def}{=}$
  A *set* Λ with the two compositions *addition* $+$ and *multiplication* $\cdot$.
  $(\Lambda, +)$ must give a *commutative group*.
  The *multiplication* must be *associative* and have a *neutral element*.
  Multiplication must be *distributive* w.r.t. *addition*. ⟨def. (1.12) p. 175 ∈ [1]⟩

  - *Notation*:

0_Λ or 0:	The *neutral element* for *addition*.
1_Λ or 1:	The *neutral element* for *multiplication*.
$-\lambda$:	The *opposite element* of λ w.r.t. $+$.

  - *All rules* for $\lambda, \mu, \nu \in \Lambda$:

$\lambda + \mu = \mu + \lambda$	a0
$(\lambda + \mu) + \nu = \lambda + (\mu + \nu)$	a1
$\lambda + 0 = \lambda$	a2
$\lambda + (-\lambda) = 0$	a3
$(\lambda\mu)\nu = \lambda(\mu\nu)$	m1
$\lambda 1 = 1\lambda = \lambda$	m2
$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu$, $(\lambda + \mu)\nu = \lambda\nu + \mu\nu$	am

- **A *commutative ring*** $(\Lambda, +, \cdot) \overset{def}{=}$
  a *ring* $(\Lambda, +, \cdot)$ where *multiplication* $\cdot$ is *commutative*. ⟨def. (1.12) p. 175 ∈ [1]⟩

- The following hold for a *ring* $(\Lambda, +, \cdot)$ with $\lambda, \mu \in \Lambda$: ⟨(1.2.1 p. 175 ∈ [1]⟩
  $0\lambda = \lambda 0 = 0$
  $(-\lambda)\mu = \lambda(-\mu) = -\lambda\mu$
  $(-1)\mu = \mu(-1) = -\mu$

- **An *invertible element*** λ a.k.a. **a *unit* in a *ring*** $(\Lambda, +, \cdot) \overset{def}{=}$
  a λ which is *invertible* w.r.t. *multiplication*. I.e. $\exists \lambda^{-1} : \lambda^{-1}\lambda = \lambda\lambda^{-1} = 1$.
  λ^{-1} is called **the *inverse element* for** λ and is *unique*.
  The *invertible elements* of Λ forms a *group*, called Λ^*.
  ⟨(1.3) p. 176 ∈ [1]⟩

- **A *subring* Δ of a ring Λ** $\overset{def}{=}$
  a subset $\Delta \subseteq \Lambda$, which is *stable* w.r.t. $+$, $-$ and $\cdot$,
  and where $0, 1 \in \Delta$. ⟨(1.4) p. 176 ∈ [1]⟩
  Notice: At least $1 \in \Delta$ must hold at the University of Copenhagen :-)

- Δ is a *subring* of the ring Λ if: ⟨(1.4) p. 176 ∈ [1]⟩
  Δ is *stable* under *addition* and *multiplication* and $-1_\Lambda \in \Delta$.

- A *subring* is a *ring* in iself. ⟨(1.4) p. 176 ∈ [1]⟩

3.1 Well-known Rings

- **The *zero-ring*** $\overset{def}{=} (\{0\}, +, \cdot)$.
  Here $1 = 0$, and this *only* holds for the zero-ring! $\langle$(1.5) p. 176 $\in$ [1]$\rangle$
  Note: The zero-ring is *not* a *subring* of any ring!
  (at least not at the University of Copenhagen :-)

- ***Number rings*** $\overset{def}{=}$ *sets of numbers* with the *usual + and* $\cdot$.
  E.g.: $(\mathbb{R}, +, \cdot)$ (a.k.a. $\mathbb{R}$). $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$. All are *commutative.* $\langle$(1.6) p. 176 $\in$ [1]$\rangle$
  $\mathbb{Z}$ is the *minimal ring* (except for the zero-ring).
  The *multiplicative groups* of *invertible elements*:
  $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{Z}^* = \{-1, 1\}$.
  Subring relations: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

- For fixed $n \in \mathbb{N}$: **The *ring* $\mathbb{Z}/n$ of *remainder classes* modulo n** $\overset{def}{=}$
  $\mathbb{Z}/n$ with *usual addition* and *multiplication.* $\mathbb{Z}/n$ is *commutative.*
  The *group* $(\mathbb{Z}/n)^*$ of *invertible remainder classes* is exactly
  the group of *primic remainder classes* modulo n. $\langle$(1.7) p. 177 $\in$ [1]$\rangle$

- For a *set* X and a *ring* Λ:
  The *ring* $\mathcal{F}_\Lambda(X)$ (a.k.a. $\mathcal{F}(X, \Lambda)$) of *functions* $f : X \to \Lambda$ $\overset{def}{=}$
  The set of functions $f : X \to \Lambda$ with
  function addition $(f + g)(x) = f(x) + g(x)$, neutral: $0(x) = 0$ and
  function multiplication $(fg)(x) = f(x)g(x)$, neutral: $1(x) = 1$.
  $\langle$(1.8) p. 177 $\in$ [1]$\rangle$
  More function rings:

  1. $\mathcal{C}(X)$: The *continuous real functions.*
  2. $\mathcal{C}^\infty(X)$: The *infinitely often differentialble real functions.*
  3. $\mathcal{H}(\Omega)$: The *holomorphic functions* $f : \Omega \to \mathbb{C}$ of an $\Omega \underset{open}{\subseteq} \mathbb{C}$.
  4. $\mathcal{P}ol(X)$: The *real polynomial functions* of X.
  5. $\mathcal{F}_\mathbb{R}(\{1, \ldots, n\})$: $\mathbb{R}^n$, i.e. *n-tuples.*
  6. $\mathcal{F}_\mathbb{R}(\mathbb{N})$: $\mathbb{R}^\mathbb{N}$, i.e. all *real number sequences.*

  Subring relations: $\mathcal{P}ol(X) \subseteq \mathcal{C}^\infty(X) \subseteq \mathcal{C}(X) \subseteq \mathcal{F}_\mathbb{R}(X)$,
  $\mathcal{P}ol(\Omega) \subseteq \mathcal{H}(\Omega) \subseteq \mathcal{F}_\mathcal{C}(\Omega)$. $\langle$(1.8) p. 177 $\in$ [1]$\rangle$

- For a *ring* Λ: **$Mat_r(\Lambda)$ of $r \times r$ matrices** is a *non-commutative ring.*
  The *upper triangular matrices* $Triang_r(\Lambda)$
  (i.e. all 0 below the diagonal) is a *subring* of $Mat_r(\Lambda)$.
  The *diagonal matrices* $Diag_r(\Lambda)$ is a *subring* of $Triang_r(\Lambda)$.
  Examples:
  $Mat_r(\mathbb{Z})$, $Mat_r(\mathbb{R})$, $Mat_r(\mathbb{C})$, $Mat_r(\mathbb{Z}/n)$.
  $|Mat_r(\mathbb{Z}/n)| = n^{r^2}$.
  Multiplicative groups:
  $A \in (Mat_r(\Lambda))^* \Leftrightarrow \det A \neq 0$. $(Mat_r(\Lambda))^* = GL_r(\Lambda)$.
  Subring relations:
  $Mat_r(\mathbb{R}) \subseteq Mat_r(\mathbb{C})$. $Diag_r(\Lambda) \subseteq Triang_r(\Lambda) \subseteq Mat_r(\Lambda)$.
  $\langle$(1.9) p. 177 $\in$ [1]$\rangle$

- Power rules for *ring* Λ: $\langle$(1.10) p. 178 $\in$ [1]$\rangle$

  1. $n\lambda \stackrel{def}{=} \begin{cases} \overbrace{\lambda + \cdots + \lambda}^{n\ times} & , \text{for } n > 0 \\ 0_\Lambda & , \text{for } n = 0 \\ (-n)(-\lambda) & , \text{for } n < 0 \end{cases}$
  2. $1\lambda = \lambda = 1_\Lambda \lambda$
  3. $(n+m)\lambda = n\lambda + m\lambda$ $\langle$power rule (1) $\in$ [1]$\rangle$
  4. $(nm)\lambda = n(m\lambda)$ $\langle$power rule (2) $\in$ [1]$\rangle$
  5. $n(\lambda + \mu) = n\lambda + n\mu$ $\langle$power rule (3) $\in$ [1]$\rangle$
  6. $\lambda(n1_\Lambda) = (n1_\Lambda)\lambda = n\lambda$ $\langle$(1.10.1) p. 178 $\in$ [1]$\rangle$

- **The *characteristic* $char(\Lambda)$ of the ring Λ** $\stackrel{def}{=}$ $\langle$(1.10) p. 178 $\in$ [1]$\rangle$
  $char(\Lambda) \stackrel{def}{=} \begin{cases} |1_\Lambda| & , \text{if this is } \textit{finite} \text{ (the } \textit{order} \text{ of } 1_\Lambda \text{ in the } \textit{group } (\Lambda, +)) \\ 0 & , \text{otherwise} \end{cases}$

- $char(\Lambda) = 1 \Leftrightarrow \Lambda = \{0\}$ (i.e. $1_\Lambda = 0_\Lambda$). $\langle$(1.10) p. 178 $\in$ [1]$\rangle$

- **The *prime ring* of Λ** $\stackrel{def}{=}$
  $\{n1_\Lambda \mid n \in \mathbb{Z}\}$. It is a *commutative subring* of Λ. $\langle$(1.10) p. 178 $\in$ [1]$\rangle$

- **The *zero-rule* for a ring Λ** $\stackrel{def}{=}$ $\langle$(1.11) p. 179 $\in$ [1]$\rangle$
  $\lambda\mu = 0 \Rightarrow \lambda = 0$ or $\mu = 0$. Equivalently: $\lambda \neq 0$ and $\mu \neq 0 \Rightarrow \lambda\mu \neq 0$.

- **The ring Λ is an *integrity area*** $\stackrel{def}{=}$ $\langle$(1.11) p. 179 $\in$ [1]$\rangle$
  The *zero-rule holds* for Λ and $\Lambda \neq \{0\}$.

- **The ring Λ is a *half field* $\langle$ DK: skævlegeme $\rangle$** $\stackrel{def}{=}$ $\langle$(1.11) p. 179 $\in$ [1]$\rangle$
  All $\lambda \neq 0$, $\lambda \in \Lambda$ are *invertible* and $\Lambda \neq \{0\}$.

- **The ring Λ is a *field* $\langle$ DK: legeme $\rangle$** $\stackrel{def}{=}$ $\langle$(1.11) p. 179 $\in$ [1]$\rangle$
  Λ is a *commutative half field*.

- Λ is a *half field* $\Rightarrow$ Λ is an *integrity area*. $\langle$(1.12)(1) p. 179 $\in$ [1]$\rangle$

- Λ is an *integrity area* $\Rightarrow$ $char(\Lambda)$ is either 0 or a *prime*.
  Holds in particular for a *half field* as well. $\langle$(1.12)(2) p. 179 $\in$ [1]$\rangle$

- For *integrity area* Λ: $\langle$(shortening rule) (1.12)(3) p. 179 $\in$ [1]$\rangle$
  $\forall \lambda \neq 0, \lambda \in \Lambda : (\lambda\mu = \lambda\nu \Rightarrow \mu = \nu)$.

- If Λ is a *ring* with p elements, where p is a *prime*, then
  Λ is a *field* and except for element names, $\Lambda = \mathbb{Z}/p$.
  $\mathbb{Z}/p$ is also denoted $\mathbb{F}_p$, but *only* when p is a *prime*. $\langle$thm. (1.14) p. 180 $\in$ [1]$\rangle$

- For a *ring* Λ and $\lambda \in \Lambda$ we define: $\langle$def. (1.16) p. 180 $\in$ [1]$\rangle$

  1. λ **is *involutoric*** $\stackrel{def}{=} \lambda^2 = 1_\Lambda$. Equivalently: $(\lambda - 1)(\lambda + 1) = 0$
  2. λ **is *idempotent*** $\stackrel{def}{=} \lambda^2 = \lambda$. Equivalently: $\lambda(\lambda - 1) = 0$.
  3. λ **is *nilpotent*** $\stackrel{def}{=} \exists N \in \mathbb{N} : \lambda^N = 0_\Lambda$.

  If the *zero-rule* holds in Λ: ± 1 are the *only involutoric* elements,
  0 and 1 are the *only idempotent* elements and 0 the *only nilpotent* element.
  Another example: *Geometric projections* are *idempotent*.

Examples

- The *zero-ring* $\{0\}$ has *characteristic* 1 and is *not* an *integrity area* and *not* a *field*. ⟨(1.13)(0) p. 179 ∈ [1]⟩
- *Number rings* have 1 as *neutral element* for *multiplication* and $\forall n \in \mathbb{Z} : n1 = n$. ⟨(1.13)(1) p. 179 ∈ [1]⟩
  So, any number ring has *characteristic* 0 and *prime ring* $\mathbb{Z}$.
  All number rings are *integrity areas* and $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are *fields*.
- A *function ring* R which is a *subring* of $\mathcal{F}(X, \mathbb{C})$ has the *constant* 1-function as 1-element.
  $char(R) = 0$ unless $X = \emptyset$.
  The *prime ring* consists of the *constant functions* with *integer values*.
  A function ring is normally *not* an *integrity area*. ⟨(1.13)(2) p. 179 ∈ [1]⟩
- The *neutral mult.* element of $Mat_r(\mathbb{R})$ is the *identity matrix* 1_r.
  $n1_r$ is the *scaling matrix* with all ns in the *diagonal*.
  The *prime ring* consists of these *integer scaling matrices*.
  $Char(Mat_r(\mathbb{R})) = 0$.
  $Mat_r(\mathbb{R})$ is *not* an *integrity area* for $n \geq 2$. ⟨(1.13)(3) p. 179 ∈ [1]⟩
- For $\mathbb{Z}/n, n \geq 1$, the *neutral multiplication* element $1_{\mathbb{Z}/n}$ is $[1]_n$.
  $k1_{\mathbb{Z}/n} = [k]_n$. $char(\mathbb{Z}/n) = n$.
  The *prime ring* of $\mathbb{Z}/n$ is the *whole ring* $\mathbb{Z}/n$.
- FIXME: Move to later?
  $\{n1_\Lambda \mid n \in \mathbb{Z}\} \cong \begin{cases} \mathbb{Z}/n & \text{, for } n = char(\Lambda) < \infty \\ \mathbb{Z} & \text{, otherwise} \end{cases}$

3.2 Ideal and Quotient Ring

Premises: R **is a** ***commutative ring***.

- $\mathcal{A} \subseteq R$ **is an** ***ideal*** **in** $R \stackrel{def}{=}$
  $(\mathcal{A}, +)$ is a *subgroup* of $(R, +)$ and $\forall r \in R, a \in \mathcal{A} : ra \in \mathcal{A}$.
- ***Trivial ideals*** **in** $R \stackrel{def}{=} R$ and $\{0\}$.
- $\mathcal{A} \subseteq R$ **is a** ***genuine ideal*** $\stackrel{def}{=}$
  $\mathcal{A}$ is an *ideal* and $\{0\} \subset \mathcal{A} \subset R$. (i.e.: $\mathcal{A} \neq \{0\}$ and $\mathcal{A} \neq R$).
- Example: For *field* L:
  The *only subideals* of L are $\{0\}$ and L.
- Example: $R = \mathbb{R}^{\mathbb{N}}$.
  $I = \{(a_1, a_2, \dots) \mid n \in \mathbb{N}$ and $(\forall i \in \{1, \dots, n\} : a_i \in R)$ and $(\forall i > n : a_i = 0)\}$.
- $R = (1)$. $\{0\} = (0)$. 1 and 0 *produces* the rings.
- The *ideals* in $\mathbb{Z}$ are *exactly* the subsets $\mathbb{Z}n, n \geq 0$.
- For $a \in R$: $Ra = \{ra \mid r \in R\}$ is an *ideal*.
- $Ra = (a)$ is a *principal ideal*.
- $R = (1)$ and $\{0\} = (0)$ are *principal ideals*.
- $I = \{(a_1, a_2, \dots) \in R^{\mathbb{N}} \mid \exists n \in \mathbb{N} : \forall i > n : a_i = 0\}$ is *not* a *principal ideal*.
- The *principal ideal* $(a) = Ra$ is the *smallest ideal* in R which *contains* a.
- ***Quotient ring*** $\stackrel{def}{=}$
  For $\mathcal{A}$ *ideal* in R. For $r \in R$: $[r] = r + \mathcal{A}$.
  Def: $[r] + [s] = [r + s]$. $[r][s] = [rs]$.
  The set of sideclasses $R/\mathcal{A}$ is a *commutative ring* with
  zero-element $[0]$ and one-element $[1]$.
- Example: $\mathbb{Z}/(n)$.
  $n > 1$: $char(\mathbb{Z}/(n)) = n$.
  $n = 1$: $char(\mathbb{Z}/(1)) = 1$. $(\mathbb{Z}/(1) = \{0\}, 1_R = 0)$
  $n = 0$: $char(\mathbb{Z}/(0)) = 0$. $(\mathbb{Z}/(0) = \mathbb{Z})$
- p **is a** ***prime ideal*** $\stackrel{def}{=}$ ⟨(2.9) p. 185 ∈ [1]⟩
  p is a *genuine ideal* and $\forall a, b \in R : ab \in p \Rightarrow a \in p \vee b \in p$.
- $m \subseteq R$ **is a** ***maximal ideal*** $\stackrel{def}{=}$ ⟨(2.9) p. 185 ∈ [1]⟩
  m is *maximal* among the *genuine ideals*.
  Equivalently: $m \subseteq \mathcal{A} \subset R \Rightarrow m = \mathcal{A}$. ⟨(2.9.2) p. 185 ∈ [1]⟩
  Equivalently: $m \subset \mathcal{A} \subseteq R \Rightarrow \mathcal{A} = R$. ⟨(2.9.3) p. 185 ∈ [1]⟩
- For $R \neq 0$:
  - (0) *prime ideal* (i.e. $ab = 0 \Rightarrow a = 0 \vee b = 0$) $\Leftrightarrow$ R *integrity area*.
  - (0) *maximal ideal* (i.e. $(0) \subset \mathcal{A} \subseteq R \Rightarrow R = \mathcal{A}$) $\Leftrightarrow$ R *field*.

- The following holds in $\mathbb{Z}$:
  - The *prime ideals* are *exactly* (0) and (p) for p *prime.*
  - The *maximal ideals* are *exactly* (p) for p *prime.*
- p *prime ideal* $\Leftrightarrow R/p$ is an *integrity area.*
- m *maximal ideal* $\Leftrightarrow R/m$ is a *field.*
- m *maximal ideal* $\Rightarrow m$ *prime ideal.*
- Example: In $\mathbb{Z}$, (0) is a *prime ideal* but *not* a *maximal ideal.*

(RNG2 p. 183-188 is missing)

3.3 Homomorphism and Isomorphism

-

(RNG3 p. 189-191 is missing)

3.4 Fraction Field

Premises: L **is a *field***.

- ***Fraction*** as^{-1} **in** $L \stackrel{def}{=}$ $\frac{a}{s} = as^{-1}$, where $a, s \in L$, $s \neq 0$. ⟨(4.1) p. 193 ∈ [1]⟩
- These rules hold for fractions: ⟨(4.1) p. 193 ∈ [1]⟩
  - $\frac{au}{su} = \frac{a}{s}$
  - $\frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}$
  - $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

(RNG4 p. 193-196 is missing)

3.5 PID and UFD

- For $a \in R$: ⟨def. (5.2) p. 197 ∈ [1]⟩
  $d \in R$ **is *divisor* in** a (notation: $d|a$) a.k.a. a **is a *multiple* of** $d \overset{def}{=}$
  $\exists q \in R : a = qd$.
  Notice: $\forall d \in R : d|0$ and 0 is *only divisor* in 0.

- For $a \in R$ and a *unit* $u \in R^*$:

  - $u|a$ and $ua|a$ by: $a = (au^{-1})u = u^{-1}(ua)$. ⟨def. (5.2) p. 197 ∈ [1]⟩
  - $d|a \equiv ud|a \equiv d|ua$. ⟨def. (5.2) p. 197 ∈ [1]⟩

- $a \in R$ **and** $a' \in R$ **are *associated*** $\overset{def}{=}$
  $\exists u \in R^* : a' = ua$. ⟨def. (5.2) p. 197 ∈ [1]⟩

- **The *trivial divisors* in** $a \overset{def}{=}$
  the *units* and the *elements associated with* a. ⟨def. (5.2) p. 197 ∈ [1]⟩
  Equivalently:
  The only *factorizations* of a as a *product* $a = bc$ are the *trivial ones*, where *one* of a and b is a *unit* (and the other thus *associated* with a).

- $q \in R$ **is *irreducible*** $\overset{def}{=}$ ⟨def. (5.2) p. 197 ∈ [1]⟩
  $q \neq 0$, $q \notin R^*$ and q has *only trivial divisors*.

- $p \in R$ **is a *prime element*** $\overset{def}{=}$ ⟨def. (5.2) p. 197 ∈ [1]⟩
  $p \neq 0$, $p \notin R^*$ and $\forall a, b \in R : p|ab \Rightarrow (p|a \vee p|b)$. ⟨def. (5.2) p. 197 ∈ [1]⟩

- $p \in R$ is a *prime element* $\Rightarrow a$ is *irreducible*. ⟨lemma (5.3) p. 198 ∈ [1]⟩

- *Properties* of *elements correspond* to
  properties of the *corresponding principal ideals*: ⟨lemma (5.3) p. 198 ∈ [1]⟩

  1. u is a *unit* $\Leftrightarrow (u) = R$
  2. a' is *associated* with $a \Leftrightarrow (a') = (a)$
  3. d is *divisor* in $a \Leftrightarrow a \in (d)$. $a \in (d) \Leftrightarrow (a) \subseteq (d)$
  4. d is a *trivial divisor* in $a \Leftrightarrow (d) = (a)$ or $(d) = R$
  5. q is *irreducible* $\Leftrightarrow$
     $q \neq 0$ and (q) is *maximal* among *genuine principle ideals*
  6. p is a *prime element* $\Leftrightarrow p \neq 0$ and (p) is a *prime ideal*

- R **is a *Principal Ideal Domain* (PID)** ⟨DK: Hovedidealområde⟩ $\overset{def}{=}$
  all ideals in R are *principal ideals*. ⟨(5.5) p. 199 ∈ [1]⟩
  How to prove that a *given integrity domain* R is a PID:
  $\forall \mathcal{A}$ *ideals* in R: $\exists d \in R : \mathcal{A} = (d)$.

- Examples of $PIDs$: ⟨(5.5), (5.6) p. 199 ∈ [1]⟩

  - $\mathbb{Z}$
  - The *polynomial ring* $L[X]$ for a *field* L

- **An *integrity domain* R is an *Euclidean Ring*** $\overset{def}{=}$ ⟨p. 199 ∈ [1]⟩
  there *exists* a function $\nu : R \to \mathbb{Z}$ which is *downwards limited* and such that $\forall d \in R, d \neq 0 : \forall a \in R : \exists q \in R : \nu(a - qd) < \nu(d)$.

- R is an *Euclidean Ring* $\Rightarrow$ R is a *PID*. ⟨p. 199 ∈ [1]⟩

- Examples of Euclidean Rings:

  – $\mathbb{Z}$ is an *Euclidean Ring*, with $\nu(a) = |a|$. ⟨p. 199 ∈ [1]⟩
  – For a *field* L, $L[X]$ is an *Euclidean Ring* with $\nu(f) = deg(f)$, where the *zero-polynomial* is given the *degree* -1. ⟨p. 199 ∈ [1]⟩

- For a PID R:

  1. $p \in R$ is *irreducible* $\Leftrightarrow$ p is a *prime element*. ⟨(5.7) p. 199 ∈ [1]⟩
  2. For *irreducible* $p \in R$: ⟨(5.7) p. 199 ∈ [1]⟩
     (a) The *Principal Ideal* (p) *produced* by p is a *maximal ideal*.
     (b) The *Quotient Ring* $R/(p)$ is a *field*.

- **A *resolution* of** $a \in R$ $\overset{def}{=}$
  $d_1 \cdots d_s = a$, where $d_1, \dots , d_s \in R$. ⟨def. (5.8) p. 200 ∈ [1]⟩

- **An *irreducible resolution* of** $a \in R$ $\overset{def}{=}$ ⟨def. (5.8) p. 200 ∈ [1]⟩
  a *resolution* $d_1 \cdots d_s = a$, where $d_1, \dots , d_s$ are *irreducible elements*.
  Note:
  Any element $a \in R$ has *trivial resolutions* $a = u(u^{-1}a)$, where $u \in R^*$.
  So, for an *irreducible resolution* $q_1 \cdots q_s = a$,
  each q_i *only* has *trivial resolutions*.

- **A *prime resolution* of** $a \in R$ $\overset{def}{=}$ ⟨def. (5.8) p. 200 ∈ [1]⟩
  a *resolution* $d_1 \cdots d_s = a$, where $d_1, \dots , d_s$ are *prime elements*.

- *Prime resolutions* are *unique* in the following sense:
  If $p_1, \dots , p_s, q_1, \dots , q_t$ are *prime elements* in R and
  the *product* $p_1 \cdots p_s$ is *associated* with the *product* $q_1 \cdots q_t$, then
  $s = t$ and after *suitable permutation* of the q_j,
  q_i is *associated* with p_i for all $i \in \{1, \dots , s\}$. ⟨lemma (5.9) p. 200 ∈ [1]⟩

- If an $a \in R$ has a *prime resolution* $p_1 \cdots p_s = a$,
  then it is *unique* in the sense that s is predetermined and each factor (except for permutation and association) is uniquely determined.
  This does *not hold* for *irreducible resolutions* in general. ⟨(5.10) p. 200-201 ∈ [1]⟩

- For *integrity domain* R we say that:

  – ***Irreducible resolutions* are *unique* in** R $\overset{def}{=}$ ⟨(5.10) p. 200-201 ∈ [1]⟩
    uniqueness of *irreducible resolutions* hold as for *prime resolutions*.
  – ***Prime resolutsions exist* for *all* elemenets** $\overset{def}{=}$ ⟨(5.10) p. 201 ∈ [1]⟩
    prime resolutions exist for *all* $a \in R$, where $a \neq 0$ and $a \notin R^*$.
  – ***Irreducible resolutsions exist* for *all* elemenets** $\overset{def}{=}$
    irreducible resolutions exist for *all* $a \in R$, where $a \neq 0$ and $a \notin R^*$.
    ⟨(5.10) p. 201 ∈ [1]⟩

  Note: *Irreducible resolutions* are *not* necessarily *unique*.

- For *integrity domain* R:
  - R **is a *Unique Factorization Domain*** ⟨DK: Faktoriel Ring⟩ $\overset{def}{=}$ *prime resolutions exist* for *all* elements. ⟨def. (5.12) p. 202 ∈ [1]⟩
  - The following are *equivalent*: ⟨thm. (5.11) p. 201 ∈ [1]⟩
    1. (a) *Irreducible resolutions exist* for *all* elements and
       (b) *irreducible resolutions* are *unique*.
    2. (a) *Irreducible resolutions exist* for *all* elements and
       (c) *any irreducible element* in R is a *prime element*.
    3. *Prime resolutions exist* for *all* elements.
    4. R is a *UFD*. ⟨def. (5.12) p. 202 ∈ [1]⟩

    Note: (a) is usually easier to realize than (b) or (c).
    E.g. if we can continue to reduce an element and the ring ensures that this process has to terminate at some point. ⟨def. (5.12) p. 202 ∈ [1]⟩

- Examples of *UFD*:
  - $\mathbb{Z}$. The *primes* in $\mathbb{Z}$ *except* from *signs* are the *irreducible elements*. The *Fundamental Theorem of Arithmetics* gives the *uniqueness* of *irreducible elements*. ⟨def. (5.12) p. 202 ∈ [1]⟩

- For a ring R where *irreducible resolutions* does *not* always exist for all elements:
  There *exists* a sequence of elements $a_1, a_2, \ldots$ in R such that a_{i+1} is a *non-trivial divisor* in a_i for all $i \in \mathbb{N}$. ⟨lemma (5.13) p. 202 ∈ [1]⟩

- For *integrity domain* R:
  If there is a given function $\nu : R \to \mathbb{Z}$ which is *downwards limited* and where for all $a \neq 0$ in R and all *non-trivial divisors* a' in a we have $\nu(a') < \nu(a)$,
  then *irreducible resolutions exist* for *all* elements in R. ⟨rem. (5.14) p. 202 ∈ [1]⟩

- Any *PID* is a *UFD*. ⟨thm. (5.15) p. 203 ∈ [1]⟩

- Examples:

Ring	Units	More comments
$\mathbb{Z}$	$\{\pm 1\}$ ⟨ex. (5.16) p. 203 ∈ [1]⟩	*Calculating except association* means *calculating except sign.* *Positive irreducible elements*: The *prime numbers.* *PID* (and thus also *UFD*). The *primes* are also the *prime elements* (because of *UFD*).
$L[X]$ (for *field* L)	*Constant polynomials* (*not zero-polynomial*) ⟨ex. (5.16) p. 203-204 ∈ [1]⟩	*Calculating except association* means *calculating except multiplication* with a *constant* $c \neq 0$. Any *non-zero polynomial* is thus *associated* with *exactly one normed polynomial.* *PID* (and thus also *UFD*). *Irreducibility* depends on L (see below).

- Polynomial irreducibility examples:
  - Usually all *1. deg. polynomials* are *irreducible.* ⟨ex. (5.16) p. 204 ∈ [1]⟩
  - A polynomial with *root* a is *divisable* by $X - a$. ⟨ex. (5.16) p. 204 ∈ [1]⟩
  - A polynomial of degree 2 or 3 is *irreducible* ⇔ it *has no roots.* ⟨ex. (5.16) p. 204 ∈ [1]⟩
  - $\mathbb{C}[X]$: *Any* polynomial of degree ≥ 1 has a *complex root.*
    Any polynomial of degree ≥ 2 is *reducible.* ⟨ex. (5.16) p. 204 ∈ [1]⟩
  - $\mathbb{R}[X]$: All irreducible polynomials: ⟨ex. (5.16) p. 204 ∈ [1]⟩
    1. degree polynomials and 2. degree polynomials *without real roots*,
    i.e.: $(X - a)^2 + b^2$, for $b \neq 0$.
  - $\mathbb{Q}[X]$: There *exist irreducible polynomials* of *any degree* ≥ 1.
    E.g.: All $X^n - 2$, for $n \in \mathbb{N}$. ⟨ex. (5.16) p. 204 ∈ [1]⟩
- *R UFD* ⇒ *R[X] UFD.* ⟨rem. (5.17) p. 204 ∈ [1]⟩
- *R UFD* ⇒ $R[X_1, \ldots, X_r]$ *UFD.* ⟨rem. (5.17) p. 204 ∈ [1]⟩
- For a *UFD R*:
  Represenation system $\mathcal{P}$ for the *prime elements* $\stackrel{def}{=}$ ⟨rem. (5.18 ∈ [1]⟩
  a *set* $\mathcal{P}$ of *prime elements* such that *each prime element* in R is *associated* with *exactly one prime element* in $\mathcal{P}$. The following holds:
  1. *Each prime element* $q \in R$ has a representation $q = ur$ with *unique* $u \in R^*$ and *unique* $r \in \mathcal{P}$. ⟨rem. (5.17) p. 204 ∈ [1]⟩
  2. For a *prime resolution* $q_1 \cdots q_s = a$ of $a \in R$, $a \neq 0$:
     We can *replace each factor* q_i with its
     unique representation $q_i = u_i p_i$ for $u_i \in R^*$, $p_i \in \mathcal{P}$.
     We can then *group duplicate primes* and *group all units* into *one unit* to get the ***unique prime resolution***:
     $up_1^{\alpha_1}, \ldots, p_r^{\alpha_r} = a$. ⟨rem. (5.17) p. 204-205 ∈ [1]⟩
     Also written: $a = u \prod_{p \in \mathcal{P}} p^{\alpha_p}$, where *only finitely many* $\alpha_p \neq 0$.
  3. For prime resolutions $u \prod_{p \in \mathcal{P}} p^{\alpha_p} = a$ and $v \prod_{p \in \mathcal{P}} p^{\delta_p} = d$ of $a \neq 0$ and $d \neq 0$ we have:
     $d | a \Leftrightarrow (\forall p \in \mathcal{P} : \delta_p \leq \alpha_p)$. ⟨rem. (5.17) p. 205 ∈ [1]⟩
  4. The *number* of *divisors* in a with *prime resolution* $u \prod_{p \in \mathcal{P}} p^{\alpha_p} = a$ *"except for association"* is:
     $\prod_{p \in \mathcal{P}} (\alpha_p + 1)$. ⟨rem. (5.17) p. 205 ∈ [1]⟩
     ($\alpha_p + 1$ is the number of exponents δ_p where $0 \leq \delta_p \leq \alpha_p$).

Greatest Common Divisor

Premises: **For the *integrity domain* R:**

- $d \in R$ **is *greatest common divisor* of** $a, b \in R$ $(d = gcd(a, b)) \stackrel{def}{=}$
  d is a *common divisor* for a and b (i.e. $d|a$ and $d|b$) and
  any other divisor c in a and b is *divisor* in d.
  For $a = 0$, $gcd(a, b) = b$. ⟨rem. (5.19) p. 205 ∈ [1]⟩

- Note: *Greatest common divisor* does *not necessarily exist* and may *not* necessarily follow any *ordering* of R. ⟨rem. (5.19) p. 205 ∈ [1]⟩

- *Greatest common divisor* is *unique, except* for *association.* ⟨rem. (5.19) p. 205 ∈ [1]⟩

- R is *UFD* $\Rightarrow$ *greatest common divisor always exists.* ⟨rem. (5.19) p. 205 ∈ [1]⟩

- R is *PID* $\Rightarrow$ the *greatest common divisor* $d \in R$ of $a, b \in R$
  can be written as:
  $d = xa + yb$ for some $x, y \in R$. ⟨rem. (5.19) p. 206 ∈ [1]⟩

- R is an *Euclidean Ring* $\Rightarrow$ *greatest common divisor*
  can be found by a generalized version of *Euklid's Algorithm.* ⟨rem. (5.19) p. 206 ∈ [1]⟩

3.6 Quadratic Number Rings

-

(RNG6 p. 207-223 is missing)

4 Polynomials

Premises: R **is a *commutative ring*.**

- **A *polynomial* f of R** $\stackrel{def}{=}$
  a *sequence* $f = (f_1, f_2, ...)$ of *elements* $f_i \in R$, such that
  only finitely many $f_i \neq 0$.
  So it holds that: $\exists n \in \mathbb{N} : \forall i > n : f_i = 0$. ⟨(1.1) p. 225 ∈ [1]⟩
  Notation: $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, where the $a_i \in R$.
  It represents the polynomial $f = (a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$.
  An a_iX^i is called a ***term* of the polynomial with *coefficient*** a_i and
  a_0 is called the ***constant term***.
  We omit the terms where $a_i = 0$ and the $a_i = 1$.

- **A *polynomial function*** $\stackrel{def}{=}$ a *function* given by the *form* of a *polynomial*.

- **A *constant polynomial*** $\stackrel{def}{=}$ $f = (a, 0, 0, 0, \ldots)$ for $a \in R$. ⟨(1.1) p. 225 ∈ [1]⟩

- **The *zero-polynomial*** $\stackrel{def}{=}$ $0 = (0, 0, 0, 0, \ldots)$. ⟨(1.1) p. 225 ∈ [1]⟩

- **The *degree* $deg(f)$ of a polynomial** $f = (a_0, a_1, \ldots)$ $\stackrel{def}{=}$
  The *biggest* $i \geq 0$ such that $a_i \neq 0$.
  The *degree* $deg(0)$ of the *zero-polynomial* is $-\infty$. ⟨(1.1) p. 226 ∈ [1]⟩

- **The *leading coefficient* of a polynomial** $f = (a_0, a_1, \ldots)$ $\stackrel{def}{=}$
  a_i when $deg(f) = i$. ⟨(1.1) p. 226 ∈ [1]⟩

- **A *normed polynomial*** f $\stackrel{def}{=}$
  the *leading coefficient* of f is 1. ⟨(1.1) p. 226 ∈ [1]⟩

- For *polynomials* $f = (f_0, f_1, \ldots)$, $g = (g_0, g_1, \ldots)$:
  - ***Polynomial sum*** $f + g$ $\stackrel{def}{=}$ $(f_0 + g_0, f_1 + g_1, \ldots)$.
    The *coefficients* are 0 from index i where $i > deg(f), i > deg(g)$,
    so the *sum* is a *polynomial*. ⟨(1.5) p. 227 ∈ [1]⟩
  - ***Polynomial product*** fg $\stackrel{def}{=}$ $(\sum_{j+k=0} f_jg_k, \sum_{j+k=1} f_jg_k, \ldots)$.
    The *coefficients* are 0 from index i where $i > deg(f) + deg(g)$,
    so the *product* is a *polynomial*. ⟨(1.5) p. 227 ∈ [1]⟩

- **The *polynomial ring* $R[X]$ of the *variable* X** $\stackrel{def}{=}$
  the set of *polynomials* with *coefficients* in R with
  polynomial addition and *polynomial multiplication*.
  ⟨(1.1) p. 226, (1.5) p. 227 ∈ [1]⟩

- $R[X]$ is *commutative*. ⟨(1.5) p. 227 ∈ [1]⟩

- The *constant polynomials* are a *subring* of $R[X]$,
  which can be *identified* with the *ring* R. ⟨(1.5) p. 227 ∈ [1]⟩

- 0 is the *constant* 0 polynomial: $(0, 0, 0, \ldots)$.
  1 is the *constant* 1 polynomial: $(1, 0, 0, \ldots)$. ⟨(1.5) p. 227 ∈ [1]⟩

- Some *polynomial equations*: ⟨(1.6) p. 227-228 ∈ [1]⟩
  - $(1+X+\cdots+X^{n-1})(X-1) = X^n - 1$.
  - $(1+X)^m = \begin{pmatrix} m \\ i \end{pmatrix} X^i$.
  - In $\mathcal{C}(\mathbb{R})[X]$: $(1+\cos^2 tX)(1-\sin^2 tX) = 1+\cos(2t)X - \frac{1}{4}\sin^2(2t)X^2$.
- For polynomials $f, h \in R[X]$: ⟨(1.7) p. 228 ∈ [1]⟩
  1. $deg(f+g) \leq \max\{deg(f), deg(g)\}$. The two sides are *equal* $\Leftrightarrow$
     $deg(f) \neq deg(g)$ or
     $deg(f) = deg(g)$ and *leading coefficients* of f and g are *not opposite*.
  2. $deg(fg) \leq deg(f) + deg(g)$.
     The two sides are *equal* $\Leftrightarrow$
     the *product* of the *leading coefficients* is *not zero*.
     In particular, if *one* of f or g is *normed*, then the 2 sides are *equal*.
- For *integrity area* R, the following holds: ⟨(1.8) p. 228 ∈ [1]⟩
  1. $\forall f, g \in R[X] : deg(fg) = deg(f) + deg(g)$.
  2. $R[X]$ is an *integrity area*.
  3. The *invertible polynomials* of $R[X]$ are
     exactly the *invertible constants* in R.
- Some polynomial integrity areas: ⟨(1.9) p. 228-229 ∈ [1]⟩

Int. Area	Invertible Polynomials
$\mathbb{Z}[X]$	± 1
$\mathbb{Q}[X]$	$\{a \in \mathbb{Q} \mid a \neq 0\}$
$L[X]$, for *field* L	$\{a \in L \mid a \neq 0\}$
$\mathbb{R}[X]$	
$\mathbb{C}[X]$	
$\mathbb{F}_p[X] = (\mathbb{Z}/p)[X]$, for *prime* p	
$\mathbb{Z}/n$, for certain n	harder to find for each n

- For a *subring* R of a *commutative ring* S:
  Polynomials with *coefficients* in R can be considered
  polynomials with *coefficients* in S. ⟨rem. (1.10) p. 229 ∈ [1]⟩
- Subring relations: $\mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$. ⟨rem. (1.10) p. 229 ∈ [1]⟩
- For given *ring homomorphism* $\phi : R \to S$, where S *commutative*:
  For polynomial $f \in R[X]$: $\phi(f) \in S[X]$ is the polynomial given by
  replacing the *coefficients* by their *images* through ϕ: ⟨rem. (1.10) p. 229 ∈ [1]⟩
  $f = a_n X^n + \cdots + a_1 X + a_0 \Rightarrow$
  $\phi(f) = \phi(a_n)X^n + \cdots + \phi(a_1)X + \phi(a_0)$.
  $f \mapsto \phi(f) : R[X] \to S[X]$ is **the *ring homomorphism indiced* by** ϕ.
  Example, for $d \in \mathbb{N}$: ⟨rem. (1.10) p. 229 ∈ [1]⟩
  $\phi(a) = [a] : \mathbb{Z} \to \mathbb{Z}/d$ induces: $f \mapsto \phi(f) : \mathbb{Z}[X] \to (\mathbb{Z}/d)[X]$.
- ***Polynomial* of *several variables*** $R[X_1, \ldots, X_n] \stackrel{def}{=}$
  $R[X_1, \ldots, X_{n-1}][X_n]$. ⟨(1.11) p. 229-230 ∈ [1]⟩

4.1 Division of Polynomials

Premises: R **is a *commutative ring***.

- *Polynomial division* and *remainder* theorem: ⟨(2.1) p. 231 ∈ [1]⟩
  For a given *normed polynomial* $d \in R[X]$:
  For *any polynomial* $f \in R[X]$,
  there *exists unique polynomials* $q, r \in R[X]$ such that:
  $f = qd + r$ and $deg(r) < deg(d)$. r *may* be the *zero-polynomial.*

- For *integrity domain* R:
  - **A *polynomial* $d \in R[X]$ is *divisor* in $f \in R[X]$** $\stackrel{def}{=}$
    $\exists q \in R[X] : qd = f$. ⟨def. (2.2) p. 231 ∈ [1]⟩
    Divisors in f thus correspond to *factorizations* of f as 2 polynomials.
  - A *normed polynomial* $d \in R[X]$ is *divisor* in $f \in R[X]$ $\Leftrightarrow$
    division of f by d gives remainder polynomial $r = 0$.
    ⟨(2.2) p. 231-232 ∈ [1]⟩
  - The *zero-polynomial* is *not divisor* in any polynomial $f \neq 0$,
    but *any polynomial* is divisor in 0. ⟨(2.2) p. 231-232 ∈ [1]⟩
  - ***Trivial divisors* in $f \in R[X]$** $\stackrel{def}{=}$
    constants $u \in R^*$ and *polynomials* of the *form* uf, for $u \in R^*$.
    The trivial divisors correspond to the *trivial factorizations*:
    $f = (u^{-1}f)u = u^{-1}(uf)$. ⟨(2.2) p. 232 ∈ [1]⟩
    This definition *depends* on R:
    E.g. $2 \notin \mathbb{Z}^*$ but $2 \in \mathbb{Q}^*$. ⟨ex. (2.3) p. 232 ∈ [1]⟩
  - ***Greatest Common Denominator* $d \in R[X]$ for 2 polynomials $f, g \in R[X]$** $\stackrel{def}{=}$
    d is a *common divisor* (i.e. $d|f$ and $d|g$) and
    any other common divisor d' is *divisor* in d (i.e. $d'|d$).
    The *greatest common denominator* does *not necessarily exist.*
    ⟨(2.2) p. 232 ∈ [1]⟩
  - **A *polynomial* $f \in R[X]$ is *irreducible*** $\stackrel{def}{=}$ ⟨(2.2) p. 232 ∈ [1]⟩
    The following holds:
    1. f is *not* the *zero-polynomial.*
    2. f is *not* an *invertible constant.*
    3. f has *only trivial divisors.*

    So, f is *reducible* $\Leftrightarrow$
    $f = gh$, where g and h are polynomials of *degree less than* f *or*
    f or g is a *constant* which is *not invertible* in R.
    This definition depends on R.
    E.g. $X^2 - 2$ is *irreducible* in $\mathbb{Q}[X]$,
    but in $\mathbb{R}[X]$ we have: $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$. ⟨ex. (2.3) p. 232 ∈ [1]⟩

- For a *field* L:
  - We can *normate* any *non-zero polynomial* $d \in L[X]$ by $a^{-1}d$, where $a \in L$ is the *leading coefficient* of d. ⟨(2.4) p. 232 ∈ [1]⟩
  - For a *product* $h \in L[X]$, $h = qd$ we can *normate* d by $h = (aq)(a^{-1}d)$, where a is the *leading coefficient* of d. ⟨(2.4) p. 232 ∈ [1]⟩
  - So for *field* L, the theorem about *division* with *remainder* holds for *any* $d \neq 0$, $d \in L[X]$. ⟨(2.4) p. 232 ∈ [1]⟩

- *Euklid's algorthm* for finding the *greatest common divisor*:
  Let L be a *field* and let $a\ mod\ b$ return the *principal remainder* from *division* of the *polynomial* $a \in L[X]$ with $b \in L[X]$.
  Define the function *gcd* by (using Standard ML-like notation):
  fun $gcd(r_i, r_j) =$ if $deg(r_j) > 0$ then $gcd(r_j, r_i\ mod\ r_j)$ else r_i.
  Then: $gcd(f, g)$ returns the *greatest common divisor* of $f, g \in L[X]$ assuming $g \neq 0$. ⟨(2.5) p. 233 ∈ [1]⟩

- For *field* L, $f, g \in L[X]$ where $g \neq 0$:
  The *common divisors* in f and g are *exactly* the *divisors* in $gcd(f, g)$.
  Furthermore: There *exists* $p, s \in L[X]$ such that:
  $gcd(f, g) = pf + sg$ (calculate backwards in *Euklid's algorithm*).
  ⟨(2.5) p. 233 ∈ [1]⟩

- For *field* L: *Any ideal* in the *polynomial ring* $L[X]$ is a *principal ideal*.
  I.e.: $\forall \mathcal{L}$ *ideal in* $L[X] : \exists d \in L[X] : \mathcal{L} = (d)$. (I.e.: $\mathcal{L} = \{qd \mid q \in L[X]\}$).
  ⟨(2.6) p. 234 ∈ [1]⟩

4.2 Roots

Premises: R **is a *commutative ring***.

- For a *finite ring* R, it is a *finite task* to determine *roots* in R for $f \in R[X]$.
  E.g.: For $R = \mathbb{Z}/6$, there are only 6 possibilities. ⟨ex. (3.3) p. 235 ∈ [1]⟩

- The *polynomial* $f \in R[X]$ has $a \in R$ as *root* $\Leftrightarrow$
  f can be written as $f = q(X - a)$ for $q \in R[X]$. ⟨(3.4) p. 236 ∈ [1]⟩

- At the end of (3.10) p. 239 it can be concluded that irreducible polynomials in $\mathbb{R}[X]$ have degree ≤ 2.
  I.e. for $f \in \mathbb{R}[X]$ with $deg(f) > 2$, f is *reducible*.

- For $f \in R[X]$, $f \neq 0$ and $a \in R$:
  a is *double root* in $f \Leftrightarrow a$ is *root* in *both* f and f'. ⟨(3.16) p. 241 ∈ [1]⟩

(POL3 p. 235-241 is missing)

4.3 Rational Coefficients

Premises: R **is a** ***commutative ring***.

- **A** ***constant*** $d \in \mathbb{Z}$ **is** ***divisor*** **in the** ***polynomial*** $f(X) \in \mathbb{Z}[X] \stackrel{def}{=}$ there *exists* a *factorization* of the form: $f(X) = dg(X)$, for $g(X) \in \mathbb{Z}[X]$. This happens *exactly when* d is a *common divisor* for the *coefficients* of $f(X)$. ⟨(4.2) p. 243 ∈ [1]⟩

- **A** ***polynomial*** $f(X) \in \mathbb{Z}[X]$ **is** ***primitive*** $\stackrel{def}{=}$ ⟨(4.2) p. 243 ∈ [1]⟩
  1 is the *greatest common denominator* for the *coefficients* of $f(X)$.
  Equivalently: $f(X)$ can *only be factored into dg* for $d \in \{\pm 1\}$, $g \in \mathbb{Z}[X]$.
  For $f(X) \neq 0$ and d is the *greatest common denominator* of the *coefficients*, the *factorization* $f(X) = dg(X)$ makes $g(X)$ *primitive.*

- Any polynomial $f(X) \in \mathbb{Z}[X]$, where $f(X) \notin \{-1, 0, 1\}$,
  can be written as a *product* of *irreducible polynomials*:
  $f(X) = dh_1(X) \cdots h_r(X)$, where $d \in \mathbb{Z}$ and the h_i have $deg(h_i) \geq 1$.
  d can be further factored into a *sign* and a *product* of *primes*, such that $f(X)$ becomes a *product* of *irreducible polynomials* in $\mathbb{Z}[X]$.
  ⟨(4.2) p. 243-244 ∈ [1]⟩

- *Eisenstein's Irreducibility Criterium*:
  Let $h(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_0 \in \mathbb{Z}[X]$ be a *primitive polynomial.*
  If there *exists a prime* p such that p is *divisor* in $c_{n-1}, \ldots, c_0$ and
  p^2 is *not* divisor in c_0, then
  $h(X)$ is *irreducible* in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$. ⟨(4.9) p. 246 ∈ [1]⟩

(POL4 p. 243-248 is missing, but includes (4.1) - (4.2))

4.4 Adjunction of Root

Premises: R **is a *commutative ring***.

-

(POL4 p. 249-252 is missing)

References

[1] Anders Thorup. *Algebra*, Matematisk Afdeling, Københavns Universitet 1998.