## DEFINITIONS

### Groups

- **semigroup:** A set with an associative binary operation.
- **group:** A set with an associative binary operation, which has a neutral (identity) element, and every element has an inverse.
- **subgroup:** For a group $G$ and $H \subseteq G$

$$H \le G \;\Leftrightarrow\; \begin{cases} 1 \in H \\ x, y \in H \Rightarrow xy \in H \\ x \in H \Rightarrow x^{-1} \in H \end{cases} \;\Leftrightarrow\; \begin{cases} 1 \in H \\ x, y \in H \Rightarrow xy^{-1} \in H \end{cases}$$

- **generated subgroup:** For a subset $S \subseteq G$,

$$\langle S \rangle = \bigcap_{S \subseteq H \le G} H = \{\, s_1^{\varepsilon_i} s_2^{\varepsilon_2} \cdots s_m^{\varepsilon_m} \mid s_i \in S,\ \varepsilon_i = \pm 1 \,\}$$

- **normal subgroup:** $N \lhd G \;\Leftrightarrow\; N \le G$ and $g^{-1}ng \in N\ \forall n \in N$ ($\Leftrightarrow Ng = gN$ for any $g \in G$)
  ($\Leftrightarrow$ there is a homomorphism $\varphi$ from $G$ such that $N = \operatorname{Ker}\varphi$)
- **order of a group:** number of elements, $|G|$
- **order of an element:** $o(g)$ is the smallest positive integer $k$ such that $g^k = 1$. $o(g) = \infty$ if no such $k$ exists. (Equivalently, $o(g) = |\,\langle g \rangle\,|$)
- **cyclic groups:** $\langle g \rangle$ (notation: $C_n$ or $C_\infty$)
- **dihedral groups:** $D_n$ is the group of symmetries (=isometries) of a regular $n$-gon ($n$ rotations, $n$ reflections)
- **symmetric groups $S_\Omega$ and $S_n$:** $S_\Omega$ is the group of bijections $\Omega \to \Omega$ (that is, permutations of $\Omega$), where the operation is the composition from left to right. The permutations act an the right: $\omega \mapsto \omega g$.
  $S_n$ if $|\Omega| = n$, usually, $\Omega = \{\,1, 2, \ldots, n\,\}$
- **alternating group $A_n$:** the group of even permutations in $S_n$.
  $A_n \lhd S_n$, $|S_n : A_n| = 2$.
- **$GL_n(K)$:** multiplicative group of invertible $n \times n$ matrices over the field $K$
- **$SL_n(K)$:** multiplicative group of $n \times n$ matrices over $K$ with determinant 1.
  $SL_n(K) \lhd GL_n(K)$
- **cycles:** $g = (a_1 a_2 \ldots a_k) \in S_\Omega$, where $a_1, \ldots, a_k$ are distinct elements of $\Omega$. $g$ maps $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$ and $b \mapsto b$ for every other $b \in \Omega$.
- **disjoint cycle decomposition (dcd):** product of cylces with no common element (it is unique up to the order of the cycles and rotations of the cycles themselves)
- **operations with permutations in dcd:**
  product: apply the permutations from left to right
  $k$th power: take the $k$th power of each cycle in the dcd (using $k$ steps instead of one)
  inverse: substitute each cycle in the dcd with the reverse cycle
  order: the least common multiple of the cycle lengths in dcd

- **even and odd permutations:** A permutation $g$ is even
  $\Leftrightarrow$ the corresponding permutation matrix $M(g)$ has determinant 1
  $\Leftrightarrow$ $g$ can be written as a product of an even number of transpositions
  $\Leftrightarrow$ a (not necessarily disjoint) cyclic decomposition of $g$ has an even number of cycles of even length).

  A permutation is odd if it is not even.
- **transpositions:** 2-cycles
- **set product:** For $X, Y \subseteq G$: $XY := \{\, xy \mid x \in X,\ y \in Y \,\} \subseteq G$.
- **cosets:** For $H \leq G$ and $g \in G$, $Hg := H\{\, g \,\}$ is a right coset, $gH := \{\, g \,\}H$ is a left coset containing $g$.
- **index of a subgroup:** For $H \leq G$, the index $|G : H|$ is the number of right cosets (the same as the number of left cosets) of $H$ in $G$. If $G$ is finite then $|G : H| = |G|/|H|$.
- **transversal:** For $H \leq G$ a subset $R \subseteq G$ is a right transversal for $H$ if every right coset contains exactly one element of $R$ (equivalently, $G$ is the disjoint union of the cosets $Hr$ $(r \in R)$. The left transversal is defined similarly.
- **factor group:** For $N \triangleleft G$, the factor group $G/N = \{\, Ng \mid g \in G \,\}$ with the set product as operation.

  For this, $NaNb = Nab$, $N1 = N$ is the identily element, and $(Na)^{-1} = Na^{-1}$.
- **complement of a normal subgroup:** For $N \triangleleft G$, $\leq G$ is a complement of $N$ if $NH = G$ and $N \cap H = 1$ (equivalently, $H \leq G$ is a transversal for $N$)
- **homomorphism and isomorphism:** $\varphi : G \to H$ is a group homomorphism if $\varphi(gg') = \varphi(g)\varphi(g')$ for every $g, g' \in G$. A bijective homomorphism is an isomorphism.
- **kernel and image:** For a homomorphism $\varphi : G \to H$,
  $\operatorname{Ker}\varphi = \{\, g \in G \mid \varphi(g) = 1 \,\} \triangleleft G$
  $\operatorname{Im}\varphi = \{\, h \in H \mid \exists g \in G :\ \varphi(g) = h \,\} \leq H$
- **conjugation:** $g^h = h^{-1}gh$. For every $h$ conjugation by $h$ is an automorphism of $G$ (that is, isomorphism from $G$ to $G$)
- **conjugacy classes:** The conjugacy class of $g$ in $G$ is $g^G := \{\, g^h \mid h \in G \,\}$.

  $G$ is the disjoint union of its conjugacy classes.
- **conjugation of permutations:** If $g : \alpha \mapsto \beta$ then $h^{-1}gh = g^h$ maps $\alpha h$ to $\beta h$. From the dcd of $g$ we get the dcd of $g^h$ by applying $h$ on the elements of the cycles of $g$.
- **cycle structures and partitions in $S_n$:** Cycle structure: describes how many cycles and what lengths appear in the dcd of the permutation. To this belongs a partition of $n$ into a sum of positive integers, 1's belonging to fixed-points.
- **group action:** $\varphi : G \to S_\Omega$ homomorphism. Notation: $\alpha g := \alpha\varphi(g)$.
  **orbit** of $\alpha \in \Omega$: $\alpha G := \{\, \alpha g \mid g \in G \,\} \subseteq \Omega$.
  **stabilizer** of $\alpha \in \Omega$: $G_\alpha = \{\, g \in G \mid \alpha g = \alpha \,\} \leq G$.
  **set of fixed-points** of $g \in G$: $\operatorname{Fix}(g) = \{\, \alpha \in \Omega \mid \alpha g = \alpha \,\} \subseteq \Omega$.

  The group action is **transitive** if it has only one orbit, that is, for any $\alpha, \beta \in \Omega$ $\exists g \in G$: $\alpha g = \beta$.

  The group action $\varphi$ is **faithful** if $\operatorname{Ker}\varphi = 1$, that is, $g = 1$ is the only element which fixes every element of $\Omega$. In this case $G$ is isomorphic to its $\varphi$-image, so $G$ can be considered as a subgroup of $S_\Omega$, that is, a permutation group.

- **centralizer of an element** $g \in G$: $C_G(g) = \{\, x \in G \mid xg = gx \,\}$, that is, the stabilizer of $g$ with respect to the conjugation on $G$ as a group action.
  **center of the group**: $Z(G) = \{\, z \in G \mid zg = gz \ \forall g \in G \,\}$. (Note that every subgroup of $Z(G)$ is a normal subgroup of $G$.)
- For a prime $p$ a $p$-**group** is a group such that every element of $G$ has $p$-power order. A finite group is a $p$-group $\Leftrightarrow$ $|G|$ is a $p$-power.
- **direct product of groups** $G_1 \times \cdots \times G_k = \{(g_1, \ldots, g_k) \mid g_i \in G_i \ \forall i = 1, \ldots, k\,\}$ (the cartesian product of $G_1, \ldots, G_k$) with the operation acting componentwise.
  **inner characterization of the direct product:** If $N_i \lhd G$ $(i = 1, \ldots, k)$, where $N_1 \cdots N_k = G$ and $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) = 1$ for every $i$ then $G = N_1 \times \cdots \times N_k$.
- **quaternion group:** $Q = \{\, \pm 1, \pm i, \pm j, \pm k \,\}$, where multiplication by $\pm 1$ acts naturally, $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$.
  - The orders of the elements: $o(1) = 1$, $o(-1) = 2$ and all the other elements have order 4.
  - Apart from $Q$ itself, every subgroup is cyclic: $\langle i \rangle, \langle j \rangle, \langle k \rangle \cong C_4$ and their intersection is $\langle -1 \rangle \cong C_2$. Every subgroup of $Q$ is normal.
- **Sylow** $p$**-subgroups:** If $|G| = p^a m$, where $p$ is a prime and $p$ does not divide $m$, then the subgroups of order $p^a$ are the Sylow $p$-subgroups of $G$. $\mathrm{Syl}_p(G)$ is the set of Sylow $p$-subgroups of $G$.
- The **normalizer** of a subgroup $H$ in $G$ is $N_G(H) = \{\, g \in G \mid H^g = H \,\}$, where $H^g := g^{-1}Hg$. Clearly, $H \lhd N_G(H) \leq G$.
- **action on** $Syl_p(G)$ **by conjugation**: $\psi : G \to S_\Omega$, where $\Omega = \mathrm{Syl}_p(G)$, and $\varphi(g) : P \mapsto P^g$. This is a transitive action by Sylow (3).

## Rings

- **ring:** $(R, +, \cdot)$ where $(R, +)$ is an abelian group, $(R, \cdot)$ is a semigroup, and the distributivity holds: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca \ \forall a, b, c \in R$.
  A ring $R$ is a
  - **commutative ring** if $ab = ba \ \forall a, b \in R$;
  - **ring with identity** if $\exists 1 \in R$: $1r = r1 = r \ \forall r \in R$;
  - **ring with no zero divisors** if $ab = 0 \Rightarrow a = 0$ or $b = 0$;
  - **integral domain** if it is commutatative, it has an identity, and it has no zero divisors.
  - **division ring**: if it is a ring with identity where every $0 \neq r \in R$ has an inverse: $rr^{-1} = r^{-1}r = 1$.
- **field:** a commutative division ring with more than one element.
- **quaternions:** $\mathbb{H} = \{\, a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \,\}$, which is a vector space with basis $\{\, 1, i, j, k \,\}$, the product of basis elements is determined by the multiplication in the quaternion group, and this extends to the general elements by distributivity, and the property that $\lambda(uv) = (\lambda u)v = u(\lambda v)$ for $\lambda \in \mathbb{R}$ and $u, v \in \mathbb{H}$. $\mathbb{H}$ is a noncommutative division ring.
- **group algebra:** For a field $K$ and finite group $G$, $KG = \{\, \sum_{g \in G} \lambda_g g \mid \lambda_g \in K \ \forall g \in G \,\}$ is a vector space over $\mathbb{R}$ with $G$ as a basis, and the multiplication is extended from the group multiplication by using distributivity and the identities $\lambda(uv) = (\lambda u)v = u(\lambda v)$ for $\lambda \in K$ and $u, v \in KG$.

- **subring:** $S \subseteq R$ is a subring of $R$ if it is nonempty, and closed under addition, multiplication and additive inverse (or equivalently, $0 \in S$, and $S$ is closed under subtraction and multiplication). Notation: $S \leq R$
- **subring generated by a subset $T \subseteq R$:** $\langle T \rangle = \bigcap\limits_{T \subseteq S \leq R} S.$
- **ideal:** $I$ is an ideal of $R$ if it is a subring, and $\forall a \in I$, $\forall r \in R$: $ar, ra \in I$. (Equivalently, $0 \in I$, and $I$ is closed under subtraction and under multiplication by any element of $R$ from both sides.) Notation: $I \triangleleft R$.
- **ideal generated by a subset $T \subseteq R$:** $(T) = \bigcap\limits_{T \subseteq S \triangleleft R} S.$
- **principal ideal:** an ideal generated by a single element: $(a)$, where $a \in R$.
- $I \triangleleft R$ is a **maximal ideal** if $I \neq R$, and for any $I \subseteq J \triangleleft R$, $J = I$ or $J = R$.
- **factor ring:** For $I \triangleleft R$: $R/I = \{\, r + I \mid r \in R \,\}$ whith the operations:

$$\begin{aligned}(r + I) + (r' + I) &= r + r' + I\\ (r + I)(r' + I) &:= rr' + I.\end{aligned}$$

- For rings $R, S$ the map $\varphi : R \to S$ is a **ring homomomorphism** if

$$\begin{aligned}\varphi(r + r') =& \varphi(r) + \varphi(r')\\ \varphi(rs) =& \varphi(r)\varphi(r')\end{aligned} \qquad \forall r, r' \in R.$$

  - The **kernel** of $\varphi$ is $\operatorname{Ker}\varphi = \{\, r \in R \mid \varphi(r) = 0 \,\} \triangleleft R$.
  - The **image** of $\varphi$ is $\operatorname{Im}\varphi = \{\, s \in S \mid \exists r \in R : \ \varphi(r) = s \,\} \leq S$.
- $R$ is a **simple ring** if the only ideals of $R$ are $0$ and $R$.
- **direct sum of rings:** $R_1 \oplus \cdots \oplus R_k = \{(r_1, \ldots, r_k) \mid r_i \in R_i \ \forall i = 1, \ldots, k\}$ (the cartesian product of $R_1, \ldots, R_k$) with the operations acting componentwise.
  **inner characterization of the direct sum :** If $I_i \triangleleft R$ $(i = 1, \ldots, k)$,
  where $I_1 + \ldots + I_k = R$ and $I_i \cap (I_1 + \ldots + I_{i-1} + I_{i+1} + \ldots + I_k) = 0$ for every $i$,
  then $R = I_1 \oplus \ldots \oplus I_k$.
- Let $R$ be an integral domain, and $a, b \in R$
  - $a$ is a **divisor** of $b$ (in notation $a \mid b$) if $\exists c \in R$ such that $b = ac$.
  - $a$ is a **unit** in $R$ if it is invertible, that is, $\exists a' \in R$ such that $aa' = 1$.
  - $a$ is **irreducible** if $a \neq 0$, $a$ is not a unit, and
    if $a = cd$ for some $c, d \in R$ then $c$ or $d$ is a unit.
  - $d \in R$ is a **greatest common divisor** of $a$ and $b$ ($d = \gcd(a, b)$) if
    $d \mid a$ and $d \mid b$;
    whenever $c \mid a$ and $c \mid b$ for some $c \in R$ then $c \mid d$.
- An integral domain $R$ is a **euclidean ring** if there is a norm $N : R \setminus \{\, 0 \,\} \to \mathbb{N}_0$ such that

$$\forall a, b \in R,\ b \neq 0,\ \exists q, r \in R : \quad a = bq + r, \quad r = 0 \text{ or } N(r) < N(b).$$

- An integral domain $R$ is a **principal ideal domain (PID)** if every ideal of $R$ is a principal ideal, i.e.
  $\forall I \triangleleft R \ \exists a \in R : \ I = (a) = aR$
- An integral domain $R$ is a **unique factorization domain (UFD)** if every element $a \in R$, which is nonzero and not invertible, can be written as a product of irreducible

elements, and this factorization is unique up to order and multiplication by invertible elements.

**Fields**

- The **characteristic of a field $K$:**
  char $K = 0$ if $na \neq 0$ for all $0 \neq a \in K$ and $n$ positive integer,
  - char $K = p$ ($p$ prime) if $pa = 0$ for every $a \in K$.
- The **prime field** of the field $K$ is its smallest subfield (that is, the intersection of all its subfields).
  If char $K = 0$ then the prime field of $K$ is $\mathbb{Q}$,
  if char $K = p$ then the prime field of $K$ is $\mathbb{Z}_p$.
- $L|K$ is a **field extension** if $K$ is a subfield of $L$.
- The **degree of the field extension** $L|K$ is $(L : K) = \dim L_K$, that is, the dimension of $L$ as a vector space over $K$.
- Let $L|K$ be a field extension.
  - $\alpha \in L$ is **algebraic** over $K$ if $\exists 0 \neq f(x) \in K[x] :\ f(\alpha) = 0$.
  - $\alpha \in L$ is **transcendental** over $K$ if it is not algebraic.
  - The extension $L|K$ is an **algebraic extension** if every element of $L$ is algebraic over $K$.
  - For $\alpha \in L$, the **simple extension generated by** $\alpha$ is $K(\alpha) = \bigcap\limits_{K,\alpha \text{ in } M \leq L} M$, that is, the smallest subfield of $L$ which contains $K$ and the element $\alpha$. (Notation: for $\alpha_1, \ldots, \alpha_k \in L$: $K(\alpha_1, \ldots, \alpha_k)$ is the smallest subfield of $L$ containing $K, \alpha_1, \ldots, \alpha_k$. This can be obtained by a series of simple extensions.)
- **minimal polynomial:** Let $L|K$ be a field extension and $\alpha$ an algebraic element over $K$. Then $0 \neq p(x) \in K[x]$ is the minimal polynomial of $\alpha$ over $K$ if
  $p(\alpha) = 0$,
  $\deg p$ is minimal among those nonzero polynomials of $K[x]$ whose root is $\alpha$,
  the main coefficient of $p(x)$ is 1.

  (Equivalently, $p(x) \in K[x]$ is an irreducible polynomial with main coefficient 1 such that $p(\alpha) = 0$ in $L$.)
- Let $f(x) \in K[x]$ and $K \leq L$. The field $L$ is a **splitting field** for $f(x)$ if
  $f(x)$ can be written as a product of linear polynomials in $L[x]$,
  and if $\alpha_1, \ldots, \alpha_n \in L$ are all the roots of $f(x)$ then $L = K(\alpha_1, \ldots, \alpha_n)$.

## THEOREMS AND PROPOSITIONS

**Groups**

- **Disjoint cycle decomposition (dcd):** $|\Omega| < \infty \Rightarrow g \in S_\Omega$ can be written as a product of disjoint cycles and this decomposition is unique up to cyclic permutations of the elements in each cycle, and up to the order of the cycles.
- **Subgroups and orders of elements of a cyclic group:**
  **P** Every subgroup of a cyclic group is cyclic,
  and for every $0 < d \mid n$
  - a) there is exactly one subgroup of order $d$ in $C_n$;

  - ○ b) the number of elements of order $d$ in $C_n$ is $\varphi(d)$.
- ○ **Order of a permutation:** If $g = c_1 \cdots c_k$ is a dcd, and $c_i$ is of length $n_i$ then $o(g) = \mathrm{lcm}(n_1, \dots, n_k)$.
- **P Lagrange Theorem:** If $|G| < \infty$ and $H \leq G$, then $|H| \mid |G|$.
  (More generally: $|G| = |H| \cdot |G : H|$ for any $G$ and $H \leq G$.)
- ○ **Order of group and element:** If $|G| < \infty$ and $g \in G$ then $o(g) \mid |G|$.
- ○ **Order of a homomorphic image of an element:** If $\varphi : G \to H$ is a homomorphism, $g \in G$ and $o(g) < \infty$ then $o(\varphi(g)) \mid \gcd(o(g), |H|)$.
- **P Homomorphism Theorem:** If $\varphi : G \to H$ is a hom., then $G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.
- ○ **Normal subgroups and kernels:** $N \lhd G \Leftrightarrow \exists$ hom. $\varphi : G \to H$ such that $N = \operatorname{Ker}\varphi$.
- ○ **Complement of a normal subgroup** If a normal subgroup $N \lhd G$ has a complement $H \leq G$, i.e. $N \cap H = 1$ and $NH = G$, then $G/N \cong H$.
- ○ **Action of conjugation:** The conjugation by $g \in G$ is an isomorphism from $G$ to $G$, so it preserves product, inverses and orders of elements.
- ○ **Conjugacy as an equivalence relation:** $G$ is the disjoint union of its conjugacy classes.
- **P Conjugacy classes of $S_n$:** $g, h \in S_n$ are conjugate
  $\Leftrightarrow$ their cycle structures are the same
  $\Leftrightarrow$ they belong to the same partition of $n$.
- ○ $1^{st}$ **Isomorphism Theorem:** If $N \lhd G$ and $H \leq G$ then $NH/N \cong H/N \cap H$.
- ○ $2^{nd}$ **Isomorphism Theorem:** If $M \leq N \leq G$ and $M, N \lhd G$ then
  $G/N \cong (G/M)/(N/M)$.
- ○ **Order of an element in $G/N$:** for $\bar{g} := Ng \in G/N$ $o(\bar{g})$ is the smallest pos. int. $k$ such that $g^k \in N$. If no such $k$ exists then $o(\bar{g}) = \infty$.
- **P Transpositions generating $S_n$:** Every element $g \in S_n$ can be written as a product of transpositions.
- ○ **3-cycles generating $A_n$:** Every element $g \in A_n$ can be written as a product of 3-cycles.
- **P $A_n$ is simple for $n \geq 5$.**
- ○ **Normal subgroups of $S_4$:** The only normal subgroups of $S_4$ are 1 ,$V$, $A_4$ and $S_4$.
- ○ For a group action $G \to S_\Omega$:
  - ○ **Cosets of stabilizer vs. orbit:** $G_\alpha g = G_\alpha h \Leftrightarrow \alpha g = \alpha h$,
    so there is a bijection between the cosets of the stabilizer of $\alpha$ and the elements of the orbit of $\alpha$.
  - **P Orbit-stabilizer lemma:** $|G| = |G_\alpha| \cdot |\alpha G|$.
    Cor.: The cardinality of any orbit $\alpha G$ is a divisor of $|G|$.
  - **P Orbit-counting lemma:** The number of orbits of the group action is $\frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|$.
- **P Class equation:** $|G| = |Z(G)| + \sum_i |\mathcal{C}_i|$, where $\mathcal{C}_i$ are the conjugacy classes of $G$ with more than one element.
- ○ **Groups of order $p^2$ and 8:**

  - For any prime $p$ there are two groups of order $p^2$ up to isomorphism: $C_{p^2}$ and $C_p \times C_p$.
  - There are 5 groups of order 8 up to isomorphism: $C_8$, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, $D_4$ and $Q$.

**P** **Cauchy theorem:** If $p$ is a prime dividing $|G|$ then $\exists g \in G$: $o(g) = p$.

- **Direct product of cyclic groups of coprime order:** If $\gcd(m, n) = 1 \Rightarrow C_m \times C_n \cong C_{mn}$.
- **Order of elements in a direct product:** If $g = (g_1, \dots, g_k) \in G_1 \times \dots \times G_k$ then $o(g) = \operatorname{lcm}(o(g_1), \dots, o(g_k))$.
- **Krull–Schmidt theorem:** Every finite group can be written as a direct product of directly indecomposable groups, and this decomposition is unique up to order and isomorphism of the components.
- **Fundamental theorem of finite abelian groups:** Every finite abelian group can be written as a direct product of cyclic groups of prime power order, and this decomposition is unique up to order and isomorphism of the components.
- **Sylow theorems:** For a finite group $G$ and prime $p$

**P** (1) $\operatorname{Syl}_p(G) \neq \emptyset$;

(1$^+$) if $S \leq G$ and $S$ is a $p$-group then $\exists P \in \operatorname{Syl}_p(G)$: $S \leq P$;

(2) $|\operatorname{Syl}_p(G)| \equiv 1 \pmod p$;

(3) for any $P, Q \in \operatorname{Syl}_p(G)$ $\exists g \in G$: $Q = P^g$.

**P** **Number of Sylow $p$-subgroups:** $|\operatorname{Syl}_p(G)| = |G : N_G(P)|$ if $P \in \operatorname{Syl}_p(G)$.

  - Cor.: If $|G| = p^a m$ with $p$ a prime, and $p$ does not divide $m$, then $|Syl_p(G)| \equiv 1 \pmod p$ and $|\operatorname{Syl}_p(G)| \mid m$.

- **Normality of a Sylow subgroup:** For $P \in \operatorname{Syl}_p(G)$ the following are equivalent:
  (i) $P \triangleleft G$;
  (ii) $|\operatorname{Syl}_p(G)| = 1$;
  (iii) the elements of $G$ of $p$-power order form a subgroup.
- **Elements covered by Sylow $p$-subgroups:** If the Sylow $p$-subgroups are of order $p$ and $|\operatorname{Syl}_p(G)| = m$, then $G$ has exactly $m(p-1)$ elements of order $p$, and all the Sylow subgroups belonging to other primes are in the remaining part of the group.

### Rings

- **Homomorphism theorem for rings:** If $\varphi : R \to S$ is a ring homomorphism then $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

**P** **Simplicity of the matrix ring:** If $K$ is a field then $K^{n \times n}$ is a simple ring.

- **Generated ideal of a ring $R$ with identity:**
  - For a subset $S \subseteq R$ the ideal generated by $S$ is $RSR = \{\, \sum_i r_i s_i r_i' \mid r_i, r_i' \in R,\ s_i \in S \,\} \cup \{\, 0 \,\}$.
  - For an element $a \in R$, the principal ideal generated by $a$ is $(a) = RaR = \{\, \sum_i r_i a r_i' \mid r_i, r_i' \in R \,\}$.
  - If $R$ is commutative then $(a) = aR$.
- **Fields and simple rings:** Let $R$ be a commutative ring, $1 \in R$. Then
  - $R$ is a field $\Leftrightarrow$ $R$ is simple.
  - For an ideal $I \triangleleft R$, $R/I$ is a field $\Leftrightarrow$ $I$ is a maximal ideal in $R$.

**P** **Euclidean ring and PID:** If $R$ is a euclidean ring then $R$ is a PID.

○ **PID and UFD:** If $R$ is a PID then it is a UFD.

○ **Connection between arithmetic properties of elements and properties of ideals in a PID $R$**

  ○ $a \mid b \Leftrightarrow (b) \subseteq (a)$

  ○ $a$ is a unit $\Leftrightarrow (a) = R$

  ○ $\exists$ unit $c$: $a = bc \Leftrightarrow (a) = (b)$

  **P** $a$ is irreducible $\Leftrightarrow (a) \underset{max}{\lhd} R$

  ○ $d = \gcd(a, b) \Leftrightarrow (d) = (a) + (b)$

○ **Factor rings of PID's:**

  ○ For a PID $R$ and $a \in R$,
  $R/(a)$ is a field $\Leftrightarrow a$ is irreducible.

  ○ Cor.: For a field $K$ and $p(x) \in K[x]$,
  $K[x]/(p(x))$ is a field $\Leftrightarrow p(x)$ is irreducible.

**Fields**

○ **Characteristic of a field:** In the additive group $(K, +)$ of a field either every nonzero element has infinite order ($\operatorname{char} K = 0$) or there is a prime $p$ such that the order of every nonzero element is $p$ ($\operatorname{char} K = p$).

○ **Prime field:** Every field $K$ has a smallest subfield, the prime field, and it is $\mathbb{Q}$ if $\operatorname{char} K = 0$, and $\mathbb{Z}_p$ if $\operatorname{char} K = p$.

○ **Factor ring of a polynomial ring:** Let $K$ be a field, $p(x) \in K[x]$ irreducible, and $\deg p(x) = n$. Then $L = K[x]/(p(x))$ is a field, containing $K$ as a subfield, and $\alpha := x + (p(x))$ is a root of $p(x)$. Furthermore, every element of $L$ can be uniquely written as a polynomial of $\alpha$ of degree $\leq n - 1$ over $K$.

**P** **Multiplicativity theorem of degrees of field extensions:** If $K \leq L \leq M$ are fields then $(M : K) = (M : L) \cdot (L : K)$.

**P** **Simple algebraic extension:** Let $K \leq L$ and $\alpha \in L$ be algebraic over $K$ with minimal polynomial $p(x)$ of degree $n$. Then

$$K(\alpha) \cong K[x]/(p(x)),$$

and every element of $L$ can be uniquely written as a polynomial of $\alpha$ of degree $\leq n - 1$ over $K$. Consequently, $(K(\alpha) : K) = n$.

○ **Simple trancendental extension:** Let $K \leq L$ and $\alpha \in L$ be a transcendental element over $K$. Then

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f, g \in K[x],\ g(x) \neq 0 \right\},$$

where $a(\alpha)/b(\alpha) = c(\alpha)/d(\alpha) \Leftrightarrow a(x)d(x) = b(x)c(x)$.

○ **Isomorphic extensions:** If $p(x) \in K[x]$ is irreducible, and $\alpha, \beta \in L \geq K$ are roots of $p(x)$ then $K(\alpha) \cong K(\beta)$.

○ **Algebraic extensions and finite degree extensions:**

  **P** If $K \leq L$ are fields, and $(L : K) < \infty$ then the extension $L|K$ is algebraic.

  - ○ For $\alpha \in L \geq K$, the extension $K(\alpha)|K$ is algebraic $\Leftrightarrow$ $(K(\alpha) : K) < \infty$.

**P** **The field of algebraic elements:** In an extension $L|K$, if $\alpha, \beta \in L$ are algebraic then $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ and $\alpha/\beta$ are also algebraic. So the algebraic elements of $L$ over $K$ form a field.

○ **$\mathbb{A}$ is algebraically closed:** The field $\mathbb{A} \leq \mathbb{C}$ of algebraic numbers over $\mathbb{Q}$ is algebraically closed.

○ **Splitting field:** Every polynomial $f(x) \in K[x]$ has a splitting field over $K$, and it is unique up to isomorphism.

○ **The multiplicative group of a finite field:**
The multiplicative group $K^\times = (K \setminus \{ 0 \}, \cdot)$ of any finite field $K$ is cyclic.

○ **Finite fields:**

  - ○ The cardinality of any finite field is a prime-power.
    For any prime $p$ and positive integer $n$ there exists exactly one finite field of cardinality $p^n$ up to isomorphism.

**P** **Finite field as a splitting field:** If $K$ is a field of cardinality $p^n$ then $K$ is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

### Other important facts from the problem sheets

2/6, 3/3, 5, 6.a), 4/6, 5/4, 6/1, 3, 7/2, 3, 8/2, 10/1, 6, 11/ review of facts in the arithmetics of polynomials.

### Requirements for the exam

You are expected to be able to precisely state the definitions and statements learned in the course, and also to prove those denoted by **P** in the above list (some of them are substatements, altogether 20). Be able to give examples and counterexamples. There will also be problems in the topic of problem sheets 11 and 12, which were not covered in the midterm tests.