Contents

1. Groups

1.1. Group Actions. What follows is based on [Ros09, p. 99].

- Let $H \leq G$, define $X := \{xH : x \in G\}$ and consider the transitive group action

$$\begin{cases} G \times X \to X \\ (g, xH) \mapsto gxH \end{cases} \tag{1}$$

The stabilizer of $xH \in X$ is given by

$$G_{xH} = xHx^{-1} \tag{2}$$

since if $g \in xHx^{-1}$ we have $g = xhx^{-1}$ for some $h \in H$ and thus $gxH = xhx^{-1}xH = xhH = xH$ and thus $g \in G_{xH}$. Conversly, if $g \in G_{xH}$ we have $gxH = xH$ and thus $gxh = xh'$ for some $h, h' \in H$ which implies $g = xh'h^{-1}x^{-1} \in xHx^{-1}$. Thus

$$\ker \lambda = \bigcap_{xH \in X} G_{xH} = \bigcap_{x \in G} xHx^{-1}. \tag{3}$$

If $[G : H]$ is finite, then $S_X \cong S_{|X|}$ and therefore by the isomorphism theorem and Lagrange

$$[G : \cap_{x \in G} xHx^{-1}] = |G / \cap_{x \in G} xHx^{-1}| \, \big| n! \tag{4}$$

Assume G is simple and $H < G$ with finite index. Then $\bigcap_{x \in G} xHx^{-1} = \langle 1 \rangle$ since if $\bigcap_{x \in G} xHx^{-1} = G$ we have $g \in xHx^{-1}$ for every $x \in G$ which implies $g \in H$ and thus $G = H$ which contradicts $H < G$.

1.2. Symmetric Groups.

- The number n_k of k-cycles in S_n is given by

$$n_k = \frac{n!}{k(n-k)!}. \tag{5}$$

- A_n is generated by all 3-cycles.
- For $n \geq 5$, A_n is simple.

1.3. Sylow Theorems. Suppose G is a finite group and $|G| = p^r m$, where $p \nmid m$. The number n_p of p-Sylowgroups fulfills

$$n_p \mid m \qquad \text{and} \qquad n_p \in \{1 + kp : k \in \mathbb{N}_0\}. \tag{6}$$

The Sylow theorems are often used to show that a groups of a certain order cannot be simple, i.e. have no nontrivial normal subgroups. This is done by showing that there exists a unique p-Sylowgroup. Since if $H \leq G$ is of unique order, we have that $\iota_g(H) = H$ for any $g \in G$. Proving in general that a group is not simple may be difficult. But most of the time we end up having the oportunity $n_p \in \{1, n\}$ where $n \in \mathbb{N}$ where $|G| = p^r m$ and $p \nmid m$. Often the following procedure works.

Assume $n_p = n$ and let X be the set of p-Sylowgroups. Consider the group action

$$\begin{cases} G \times X \to X \\ (g, P) \mapsto gPg^{-1} \end{cases}. \tag{7}$$

This action is well defined, since generally if P is a p-Sylow group so is gPg^{-1} for any $g \in G$ since $gPg^{-1} = \iota_g(P)$ where

$$\iota_g : \begin{cases} G \to G \\ x \mapsto gxg^{-1} \end{cases} \tag{8}$$

is the so-called inner automorphism. Now if $|P| = p^r$ then $|gPg^{-1}| = p^r$ and clearly $gPg^{-1} \leq G$. Since $|X| = n$ we have $S_X \cong S_n$ as one trivially sees by considering the isomorphism

$$\iota : \begin{cases} S_n \to S_X \\ \sigma \mapsto \begin{pmatrix} x_1 & \dots & x_n \\ x_{\sigma(1)} & \dots & x_{\sigma(n)} \end{pmatrix} \end{cases} \tag{9}$$

Therefore by considering the permutation representation of the group action above

$$\lambda : \begin{cases} G \to S_X \\ g \mapsto \lambda_g \end{cases} \qquad \text{where} \qquad \lambda_g : \begin{cases} X \to X \\ P \mapsto gPg^{-1} \end{cases} \tag{10}$$

which is a homomorphism and using that the composition of homomorphisms is again a homomorphism, we get a homomorphism

$$\lambda' : G \to S_n \tag{11}$$

1.4. Direct Products.

Definition 1.1. *Suppose $H, J \trianglelefteq G$ with $H \cap J = \langle 1 \rangle$ and $G = HJ$. Then G is said to be the **internal direct product** of H and J and we have*

$$G \cong H \times J \cong J \times H. \tag{12}$$

Definition 1.2. *Let $A \leq G$, $K \trianglelefteq G$ where $G = AK$ and $A \cap K = \langle 1 \rangle$. Then G is said to be an **internal semi-direct product** of K by A, written*

$$G \cong A \rtimes K. \tag{13}$$

2. Rings

2.1. Basic Definitions, Properties and Examples.

Definition 2.1. *A commutative ring R with unity is called an **integral domain** if it has one of the following equivalent properties:*

(i) *(**Cancellation**) $zx = zy$ implies $x = y$ for any $x, y, z \in R$ with $z \neq 0$.*

(ii) *(**No divisors of zero**) $xy = 0$ implies either $x = 0$ or $y = 0$ for any $x, y \in R$.*

Definition 2.2. *A ring R with identity is called a **skew field** if $R^\times = R \setminus \{0\}$.*

Definition 2.3. *A commutative skew field is called a **field**.*

Definition 2.4. *A ring $R \neq \{0\}$ is called **simple** if (0) and R are the only ideals.*

Definition 2.5. *Let R be a commutative ring. An ideal $P \neq R$ is called a **prime ideal** if $ab \in P$ implies either $a \in P$ or $b \in P$ for $a, b \in R$.*

Proposition 2.1. *An ideal $P \neq R$ of a commutative ring R with identity is a prime ideal if and only if R/P is an integral domain.*

Definition 2.6. *An ideal $M \neq R$ is called **maximal** if there exists no ideal I such that $M \subsetneq I \subsetneq R$.*

Proposition 2.2. *Let R be a commutative ring with identity. An ideal $M \neq R$ is maximal if and only if R/M is a field.*

Definition 2.7. *An integral domain R is called a **factorial domain** or **unique factorisation domain** when the following properties hold:*

(i) *Every element $x \notin R^\times \cup \{0\}$ can be written as product of irreducible factors.*

(ii) *If $p_1 \cdots p_n = q_1 \cdots q_m$ for irreducible $p_1, \ldots, p_n, q_1, \ldots, q_m \in R$, then $n = m$ and there exists $\sigma \in S_n$ such that $p_i \sim q_{\sigma(i)}$ for $i = 1, \ldots, n$.*

Definition 2.8. *An integral domain is called a **principal ideal domain** if every ideal of R is principal.*

Theorem 2.1. *Every principal ideal domain is a factorial domain.*

Definition 2.9. *An integral domain R is called an **euclidean domain** if there is a mapping $\varphi : R \setminus \{0\} \to \mathbb{N}_0$ with the following property: To any $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.*

Example 2.1 (Euclidean Domains). Consider the ***Gaussian integers*** $\mathbb{Z}[i]$. The mapping $N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}_0$ defined by $N(z) := z\overline{z}$ is a euclidean norm.

Theorem 2.2. *Every euclidean domain is a principal ideal domain.*

Definition 2.10. *A ring R is called* ***noetherian*** *if it has one of the following equivalent properties:*

(i) *Every ascending chain $A_1 \subseteq A_2 \subseteq \dots$ of ideals A_i of R is stationary, i.e. there exists some $k \in \mathbb{N}$ such that $A_i = A_k$ for every $i \geq k$.*
(ii) *Every nonempty collection of ideals of R contains a maximal element.*
(iii) *Every ideal of R is finitely generated.*

Theorem 2.3 (Hilbert). *If R is a commutative noetherian ring with identity then $R[X]$ is noetherian.*

Example 2.2 (Rings).

(a) $\mathbb{H} := \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, w \in \mathbb{C} \right\}$ is a subring of $\mathbb{C}^{2\times 2}$ with identity.

(b) Let K be a field and $z \in K$. Then $K_z := \left\{ \begin{pmatrix} x & zy \\ y & x \end{pmatrix} : x, y \in K \right\}$ is a commutative subring of $K^{2\times 2}$.

(c) Let $d \in \mathbb{Z} \setminus \{1\}$ be square-free, i.e. if $x^2 | d$ for $n \in \mathbb{N}$ then $x = 1$. Then $\mathbb{Z}[\sqrt{d}], \mathbb{Q}[\sqrt{d}] \subseteq \mathbb{C}$ are commutative rings with identity. The mapping

$$\bar{\cdot} : \begin{cases} \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}] \\ x + y\sqrt{d} \mapsto x - y\sqrt{d} \end{cases} \tag{14}$$

is an automorphism. Furthermore, the mapping $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}$ defined by $N(z) := z\overline{z}$ is multiplicative. Moreover, for $z \in \mathbb{Z}[\sqrt{d}]$ we have

$$z \in \mathbb{Z}[\sqrt{d}]^{\times} \Leftrightarrow N(z) \in \{\pm 1\}\,. \tag{15}$$

$\mathbb{Q}[\sqrt{d}]$ is a field, whereas $\mathbb{Z}[\sqrt{d}]$ is not.

(d) Let R be a commutative ring with identity. Then

$$R[[X]] := \{f : f : \mathbb{N}_0 \to R\} \tag{16}$$

is a commutative extension ring with identity of $R[X]$. We have

$$R[[X]]^{\times} = \left\{ \sum_{i \in \mathbb{N}_0} a_i X^i : a_0 \in R^{\times} \right\}. \tag{17}$$

(e) Let R be a commutative ring with ideal A. Then

$$\sqrt{A} := \{x \in R : \exists n \in \mathbb{N} \text{ s.t. } x^n \in A\} \tag{18}$$

is an ideal in R. It holds that

$$A = \sqrt{A} \Leftrightarrow R/A \text{ does not contain any nilpotent elements} \neq 0. \tag{19}$$

Furthermore, for any prime ideal P we have $P = \sqrt{P}$ and

$$\sqrt{(0)} = \bigcap_{P \text{ prime ideal}} P. \tag{20}$$

(f) Let p be a prime number and

$$D_p := \left\{ \frac{x}{y} \in \mathbb{Q} : \gcd(x,y) = 1 \text{ and } p \nmid y \right\}. \tag{21}$$

Then D_p is a principal ideal domain.

Example 2.3 (Automorphism of Rings).

(a) Let R be an integral domain and $a \in R^\times$, $b \in R$. Then there exists a unique $\varphi \in \mathrm{Aut}(R[X])$, such that $\varphi|_R = \mathrm{id}_R$ and $\varphi(X) = aX + b$. Furthermore, if $\varphi \in \mathrm{Aut}(R[X])$ with $\varphi|_R = \mathrm{id}_R$, there are $a \in R^\times$, $b \in R$ such that $\varphi(X) = aX + b$.

(b) Let R be an integral domain and $B \in R[X]$. The mapping

$$\varepsilon_B : \begin{cases} R[X] \to R[X] \\ A \to A(B) \end{cases} \tag{22}$$

is an automorphism if and only if $\deg(B) = 1$ and the leading coefficient of B is a unit in R.

(c) Consider $\mathbb{Q}$ and $\mathbb{R}$ as rings. Then

$$|\mathrm{Aut}(\mathbb{Q})| = 1 = |\mathrm{Aut}(\mathbb{R})| \tag{23}$$

2.2. The Chinese Remainder Theorem.

Theorem 2.4 (Chinese Remainder Theorem). *Let R be a ring with identity and $A_1, \ldots, A_n$ ideals of R with $A_i + A_j = R$ whenever $i \neq j$. Then the mapping*

$$\Phi : \begin{cases} R/(A_1 \cap \cdots \cap A_n) \to R/A_1 \times \cdots \times R/A_n \\ a + A_1 \cap \ldots A_n \mapsto (a + A_1, \ldots, a + A_n) \end{cases} \tag{24}$$

is an isomorphism of rings.

Proof. Well-definedness and injectivity are easy. For surjectivity proove

$$R = A_j + \bigcap_{i \neq j} A_i \tag{25}$$

for $j = 1, \ldots, n$. □

Example 2.4 (Application of the Chinese Remainder Theorem 2.4). Consider the system of congruence equations

$$X \equiv a_1 \bmod r_1, \ldots, X \equiv a_n \bmod r_n \tag{26}$$

where $r_1, \ldots, r_n \in \mathbb{Z}$ are pairwise coprime and $a_1, \ldots, a_n \in \mathbb{Z}$. Now set

$$r := r_1 \cdots r_n \qquad \text{and} \qquad s_i := \frac{r}{r_i} \tag{27}$$

for each $i = 1, \ldots, n$ and determine $k_i \in \mathbb{Z}$ such that

$$k_i s_i \equiv 1 \bmod r_i \tag{28}$$

for each $i = 1, \ldots, n$. This can be done using the extended euclidean algorithm, i.e. since s_i and r_i are coprime, we find $t_i \in \mathbb{Z}$ such that

$$k_i s_i + t_i r_i = 1. \tag{29}$$

Then

$$k := k_1 s_1 a_1 + \cdots + k_n s_n a_n \tag{30}$$

is a solution of (26) and the set of solutions of (26) is $k + r\mathbb{Z}$.

Bibliography

[Ros09] H.E. Rose. *A Course on Finite Groups*. Universitext. Springer London, 2009. ISBN: 9781848828896. URL: https://books.google.ch/books?id=sb3PtsYlMFEC.