24 Nilpotent groups

24.1. Recall that if G is a group then

$$Z(G) = \{a \in G \ \mid \ ab = ba \text{ for all } b \in G\}$$

Note that $Z(G) \lhd G$. Take the canonical epimorphism $\pi\colon G \to G/Z(G)$. Since $Z\left(G/Z(G)\right) \lhd G/Z(G)$ we have:

$$\pi^{-1}\left(Z\left(G/Z(G)\right)\right) \lhd G$$

Define:

$$\begin{aligned} Z_1(G) :=& Z(G) \\ Z_i(G) :=& \pi_i^{-1}\left(Z\left(G/Z_{i-1}(G)\right)\right) \qquad \text{for } i > 1 \end{aligned}$$

where $\pi_i\colon G \to G/Z_{i-1}(G)$. We have $Z_i(G) \lhd G$ for all i.

24.2 Definition. The *upper central series* of a group G is a sequence of normal subgroups of G:

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \dots$$

24.3 Definition. A group G is *nilpotent* if $Z_i(G) = G$ for some i.

If G is a nilpotent group then the *nilpotency class* of G is the smallest $n \geq 0$ such that $Z_n(G) = G$.

24.4 Proposition. *Every nilpotent group is solvable.*

Proof. If G is nilpotent group then the upper central series of G

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq \ \dots \ \subseteq Z_n(G) = G$$

is a normal series.

Moreover, for every i we have

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$$

so all quotients of the upper central series are abelian. $\square$

24.5 Note. Not every solvable group is nilpotent. Take e.g. G_T. We have $Z(G_T) = \{I\}$, and so

$$Z_i(G_T) = \{I\}$$

for all i. Thus G_T is not nilpotent. On the other hand G_T is solvable with a composition series

$$\{I\} \subseteq \{I, R_1, R_2\} \subseteq G_T$$

24.6 Proposition.

1) Every abelian group is nilpotent.

2) Every finite p-group is nilpotent.

Proof.

1) If G is abelian then $Z_1(G) = G$.

2) If G is a p-group then so is $G/Z_i(G)$ for every i. By Theorem 16.4 if $G/Z_i(G)$ is non-trivial then its center $Z(G/Z_i(G))$ a non-trivial group. This means that if $Z_i(G) \neq G$ then $Z_i(G) \subseteq Z_{i+1}(G)$ and $Z_i(G) \neq Z_{i+1}(G)$. Since G is finite we must have $Z_n(G) = G$ for some G. $\square$

24.7 Definition. A *central series* of a group G is a normal series

$$\{e\} = G_0 \subseteq \ldots \subseteq G_k = G$$

such $G_i \lhd G$ and $G_{i+1}/G_i \subseteq Z(G/G_i)$ for all i.

24.8 Proposition. *If* $\{e\} = G_0 \subseteq \ldots \subseteq G_k = G$ *is a central series of* G *then*

$$G_i \subseteq Z_i(G)$$

Proof. Exercise. □

24.9 Corollary. *A group* G *is nilpotent iff it has a central series.*

Proof. If G is nilpotent then

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq \ \ldots \ \subseteq Z_n(G) = G$$

is a central series of G.

Conversely, if

$$\{e\} = G_0 \subseteq \ldots \subseteq G_k = G$$

is a central series of G then by (24.9) we have $G = G_k \subseteq Z_k(G)$, so $G = Z_k(G)$, and so G is nilpotent. □

24.10 Note. Given a group G define

$$\begin{aligned} \Gamma_0(G) :=& G \\ \Gamma_i(G) :=& [G, \Gamma_{i-1}(G)] \quad \text{for } i > 0. \end{aligned}$$

We have

$$\ldots \subseteq \Gamma_1(G) \subseteq \Gamma_0(G) = G$$

24.11 Proposition. *If* G *is a group then*

1) $\Gamma_i(G) \lhd G$ *for all* i

2) $\Gamma_{i+1}(G)/\Gamma_i(G) \subseteq Z(G/\Gamma_i(G))$ *for all* i

Proof. Exercise. □

24.12 Definition. If $\Gamma_n(G) = \{e\}$ then

$$\{e\} = \Gamma_n(G) \subseteq \ldots \subseteq \Gamma_0(G) = G$$

is a central series of G. It is called the *lower central series* of G.

24.13 Proposition. *A group* G *is nilpotent iff* $\Gamma_n(G) = \{e\}$

Proof. Exercise. □

24.14 Theorem.

1) *Every subgroup of a nilpotent group is nilpotent.*
2) *Ever quotient group of a nilpotent group is nilpotent.*
3) *If* $H \lhd G$*, and both* H *and* G/H *are nilpotent groups then* G *is also nilpotent.*

Proof. Similar to the proof of Theorem 23.6. □

24.15 Corollary. *If* $G_1, \ldots, G_k$ *are nilpotent groups then the direct product* $G_1 \times \cdots \times G_k$ *is also nilpotent.*

Proof. Follows from part 3) of Theorem 24.14. □

24.16 Corollary. *If $p_1, \dots, p_k$ are primes and P_i is a p_i-group then $P_1 \times \ldots \times P_k$ is a nilpotent group.*

Proof. Follows from (24.6) and (24.15). $\square$

24.17 Theorem. *Let G be a finite group. The following conditions are equivalent.*

1) *G is nilpotent.*
2) *Every Sylow subgroup of G is a normal subgroup.*
3) *G isomorphic to the direct product of its Sylow subgroups.*

24.18 Lemma. *If G is a finite group and P is a Sylow p-subgroup of G then*

$$N_G(N_G(P)) = N_G(P)$$

Proof. Since $P \subseteq N_G(P) \subseteq G$ and P is a Sylow p-subgroup of G therefore P is a Sylow p-subgroup of $N_G(P)$. Moreover, $P \lhd N_G(P)$, so P is the only Sylow p-subgroup of G.

Take $a \in N_G(N_G(P))$. We will show that $a \in N_G(P)$. We have

$$aPa^{-1} \subseteq aN_G(P)a^{-1} = N_G(P)$$

As a consequence aPa^{-1} is a Sylow p-subgroup of $N_G(P)$, and thus $aPa^{-1} = P$. By the definitions of normalizer this gives $a \in N_G(P)$. $\square$

24.19 Lemma. *If H is a proper subgroup of a nilpotent group G (i.e. $H \subseteq G$, and $H \neq G$), then H is a proper subgroup of $N_G(H)$.*

Proof. Let $k \geq 0$ be the biggest integer such that $Z_k(G) \subseteq H$. Take $a \in Z_{k+1}(G)$ such that $a \notin H$. We will show that $a \in N_G(H)$.

We have

$$H/Z_k(G) \subseteq G/Z_k(G) \quad \text{and} \quad Z_{k+1}(G)/Z_k(G) = Z(G/Z_k(G))$$

If follows that for every $h \in H$ we have

$$ahZ_k(G) = (aZ_k(G))(hZ_k(G)) = (hZ_k(G))(aZ_k(G)) = haZ_k(G)$$

Therefore $ha = ahh'$ for some $h' \in Z_k(G) \subseteq H$, and so $a^{-1}ha = hh' \in H$. As a consequence $a^{-1}Ha = H$, so $a^{-1} \in N_G(H)$, and so also $a \in N_G(H)$.

□

Proof of Theorem 24.17.

1) $\Rightarrow 2)$ Let P be a Sylow p-subgroup of G. It suffices to show that $N_G(P) = G$.

Assume that this is not true. Then $N_G(P)$ is a proper subgroup G, and so by Lemma 24.19 it is also a proper subgroup of $N_G(N_G(P))$. On the other hand by Lemma 24.18 we have $N_G(N_G(P)) = N_G(P)$, so we obtain a contradiction.

2) $\Rightarrow 3)$ Exercise.

3) $\Rightarrow 1)$ Follows from Corollary 24.16.

□

25 Rings

25.1 Definition. A *ring* is a set R together with two binary operations: addition $(+)$ and multiplication $(\cdot)$ satisfying the following conditions:

1) R with addtion is an abelian group.
2) multiplication is associative: $(ab)c = a(bc)$
3) addition is distributive with respect to multiplication:

$$a(b+c) = ab + ac \qquad\qquad (a+b)c = ac + bc$$

The ring R is *commutative* if $ab = ba$ for all $a, b \in R$.

The ring R is a *ring with identity* if there is and element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$. (Note: if such identity element exists then it is unique)

25.2 Examples.

1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings with identity.

2) $\mathbb{Z}/n\mathbb{Z}$ is a ring with multiplication given by

$$k(n\mathbb{Z}) \cdot l(n\mathbb{Z}) := kl(n\mathbb{Z})$$

3) If R is a ring then

$$R[x] = \{a_0 + a_1x + \ldots + a_nx^n \mid a_i \in R,\ n \geq 0\}$$

is the ring of polynomials with coefficients in R and

$$R[[x]] = \{a_0 + a_1x + \ldots \mid a_i \in R\}$$

is the ring of formal power series with coefficients in R.

If R is a commutative ring then so are $R[x]$, $R[[x]]$. If R has identity then $R[x]$, $R[[x]]$ also have identity.

4) If R is a ring then $M_n(R)$ is the ring of $n \times n$ matrices with coefficients in R.

5) The set $2\mathbb{Z}$ of even integers with the usual addition and multiplication is a commutative ring without identity.

6) If G is an abelian group then the set $\mathrm{Hom}(G.G)$ of all homomorphisms $f\colon G \to G$ is a ring with multiplication given by composition of homomorphisms and addition defined by

$$(f+g)(a) := f(a) + g(a)$$

7) If R is a ring and G is a group then define

$$R[G] := \{ \sum_{g\in G} a_g g \mid a_g \in R,\ a_g \neq 0 \text{ for finitely many } g \text{ only } \}$$

addition in $R[G]$:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$

multiplication in $R[G]$:

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g G\right) = \sum_{g\in G}\left(\sum_{hh'=g} a_h a_{h'}\right) g$$

The ring $R[G]$ is called the *group ring* of G with coefficients in R.

25.3 Definition. Let R be a ring. An element $0 \neq a \in R$ is a *left (resp. right) zero divisor in* R if there exists $0 \neq b \in R$ such that $ab = 0$ (resp. $ba = 0$).

An element $0 \neq a \in R$ is a *zero divisor* if it is both left and right zero divisor.

25.4 Example. In $\mathbb{Z}/6\mathbb{Z}$ we have $2 \cdot 3 = 0$, so 2 and 3 are zero divisors.

25.5 Definition. An *integral domain* is a commutative ring with identity $1 \neq 0$ that has no zero divisors.

25.6 Proposition. *Let R be an integral domain. If $a, b, c \in R$ are non-zero elements such that*

$$ac = bc$$

then $a = b$.

Proof. We have $(a - b)c = 0$. Since $c \neq 0$ and R has no zero divisors this gives $a - b = 0$, and so $a = b$. $\square$

25.7 Definition. Let R be a ring with identity. An element a has a *left (resp. right) inverse* if there exists $b \in R$ such that $ba = 1$ (resp. there exists $c \in R$ such that $cb = 1$).

An element $a \in R$ is a *unit* if it has both a left and a right inverse.

25.8 Proposition. *If a is a unit of R then the left inverse and the right inverse of a coincide.*

Proof. If $ba = 1 = ac$ then

$$b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c$$

$\square$

25.9 Note. The set of all units of a ring R forms a group R^* (with multiplication). E.g.:

$\mathbb{Z}^* = \{-1, 1\} \cong \mathbb{Z}/2\mathbb{Z}$
$\mathbb{R}^* = \mathbb{R} - \{0\}$
$(\mathbb{Z}/14\mathbb{Z})^* = \{1, 3, 5, 9, 11, 13\} \cong \mathbb{Z}/6\mathbb{Z}$

25.10 Definition. A *division ring* is a ring R with identity $1 \neq 0$ such that every non-zero element of R is a unit.

A *field* is a commutative division ring.

25.11 Examples.

1) $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ are fields.

2) $\mathbb{Z}$ is an integral domain but it is not a field.

3) The ring of *real quaternions* is defined by

$$\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

Addition in $\mathbb{H}$ is coordinatewise. Multiplication is defined by the identities:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

The ring $\mathbb{H}$ is a (non-commutative) division ring with the identity

$$1 = 0 + 0i + 0j + 0k$$

The inverse of an element $z = a + bi + cj + dk$ is given by

$$z^{-1} = (a/\|z\|) - (b/\|z\|)i - (c/\|z\|)j - (d/\|z\|)k$$

where $\|z\| = \sqrt{a^2 + b^2 + c^2 + d^2}$

25.12 Proposition. *The following conditions are equivalent.*

1) $Z/n\mathbb{Z}$ *is a field.*

2) $Z/n\mathbb{Z}$ *is an integral domain.*

3) n *is a prime number.*

Proof. Exercise. $\square$

26 Ring homomorphisms and ideals

26.1 Definition. Let R, S be rings. A *ring homomorphism* is a map

$$f\colon R \to S$$

such that

1) $f(a+b) = f(a) + f(b)$
2) $f(ab) = f(a)f(b)$

26.2 Note. If R, S are rings with identity then these conditions do not guarantee that $f(1_R) = 1_S$.

Take e.g. rings with identity R_1, R_2 and define

$$R_1 \oplus R_2 = \{(r_1, r_2) \mid r_1 \in R_1, R_2\}$$

with addition and multiplication defined coordinatewise. Then $R_1 \oplus R_2$ is a ring with identity $(1_{R_1}, 1_{R_2})$. The map

$$f\colon R_1 \to R_1 \oplus R_2, \qquad f(r_1) = (r_1, 0)$$

is a ring homomorphism, but $f(1_{R_1}) \neq (1_{R_1}, 1_{R_2})$.

26.3 Note. Rings and ring homomorphisms form a category $\mathcal{R}ing$.

26.4 Proposition. *A ring homomorphism $f\colon R \to S$ is an isomorphism of rings iff f is a bijection.*

Proof. Exercise. □

26.5 Definition. If $f\colon R \to S$ is a ring homomorphism then

$$\mathrm{Ker}(f) = \{a \in R \mid f(a) = 0\}$$

26.6 Proposition. *A ring homomorphism is 1-1 iff* $\mathrm{Ker}(f) = \{0\}$

Proof. The same as for groups (4.4). □

26.7 Definition. A *subring* of a ring R is a subset $S \subseteq R$ such that S is an additive subgroup of R and it is closed under the multiplication.

A *left ideal* of R is a subring $I \subseteq R$ such that for every $a \in I$ and $b \in R$ we have $ab \in I$. A *right ideal* of R is defined analogously.

A *ideal* of R is a subring $I \subseteq R$ such that I is both left and right ideal.

26.8 Notation. If I is an ideal of R then we write $I \lhd R$.

26.9 Proposition. *If* $f\colon R \to S$ *is a ring homomorphism then* $\mathrm{Ker}(f)$ *is an ideal of* R*.*

Proof. Exercise. □

26.10 Definition. If I is an ideal of a ring R then the *quotient ring* R/I is defined as follows.

$$R/I := \text{ the set of left cosets of } I \text{ in } R$$

Addition: $(a+I)+(b+I) = (a+b)+I$, multiplication: $(a+I)(b+I) = ab+I$.

26.11 Note. If $I \lhd R$ then the map

$$\pi\colon R \to R/I, \qquad \pi(a) = a + I$$

is a ring homomorphism. It is called the *canonical epimorphism* of R onto R/I.

26.12 Theorem. *If $f\colon R \to S$ is a homomorphism of rings then there is a unique homomorphism*

$$\bar{f}\colon R/\operatorname{Ker}(f) \to S$$

such that the following diagram commutes:

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\
R/\operatorname{Ker}(f) \arrow[ur, dashed, "\bar{f}"'] &
\end{tikzcd}$$

Moreover, $\bar{f}$ is a monomorphism and $\operatorname{Im}(\bar{f}) = \operatorname{Im}(f)$.

Proof. Similar to the proof of Theorem 6.1 for groups. $\square$

26.13 First Isomorphism Theorem. *If $f\colon R \to S$ is a homomorphism of rings that is an epimorphism then*

$$R/\operatorname{Ker}(f) \cong S$$

Proof. Take the map $\bar{f}\colon R/\operatorname{Ker}(f) \to S$. Then $\operatorname{Im}(\bar{f}) = \operatorname{Im}(f) = S$, so $\bar{f}$ is an epimorphism. Also, $\bar{f}$ is 1-1. Therefore $\bar{f}$ is a bijective homomorphism and thus it is an isomorphism. $\square$

26.14 Note. Let $I, J \lhd R$. Check:

1) $I \cap J \lhd R$

2) $I + J \lhd R$ where $I + J = \{a + b \mid a \in I,\ b \in J\}$

26.15 Second Isomorphism Theorem. *If I, J are ideals of R then*

$$I/(I \cap J) \cong (I + J)/J$$

Proof. Exercise. $\square$

26.16 Third Isomorphism Theorem. *If I, J are ideals of R and $J \subseteq I$ then I/J is a ideal of R/J and*

$$(R/J)/(I/J) \cong R/I$$

Proof. Exercise. $\square$