## 24 Nilpotent groups

24.1. Recall that if $G$ is a group then

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

Note that $Z(G) \triangleleft G$. Take the canonical epimorphism $\pi: G \rightarrow G / Z(G)$. Since $Z(G / Z(G)) \triangleleft G / Z(G)$ we have:

$$
\pi^{-1}(Z(G / Z(G))) \triangleleft G
$$

Define:

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

where $\pi_{i}: G \rightarrow G / Z_{i-1}(G)$. We have $Z_{i}(G) \triangleleft G$ for all $i$.
24.2 Definition. The upper central series of a group $G$ is a sequence of normal subgroups of $G$ :

$$
\{e\}=Z_{0}(G) \subseteq Z_{1}(G) \subseteq Z_{2}(G) \subseteq \ldots
$$

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 $G$

$$
\{e\}=Z_{0}(G) \subseteq Z_{1}(G) \subseteq \ldots \subseteq Z_{n}(G)=G
$$

is a normal series.

Moreover, for every $i$ we have

$$
Z_{i}(G) / Z_{i-1}(G)=Z\left(G / Z_{i-1}(G)\right)
$$

so all quotients of the upper central series are abelian.
24.5 Note. Not every solvable group is nilpotent. Take e.g. $G_{T}$. We have $Z\left(G_{T}\right)=\{I\}$, and so

$$
Z_{i}\left(G_{T}\right)=\{I\}
$$

for all $i$. Thus $G_{T}$ is not nilpotent. On the other hand $G_{T}$ is solvable with a composition series

$$
\{I\} \subseteq\left\{I, R_{1}, R_{2}\right\} \subseteq G_{T}
$$

### 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 $Z\left(G / Z_{i}(G)\right)$ 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 $G$.
24.7 Definition. A central series of a group $G$ is a normal series

$$
\{e\}=G_{0} \subseteq \ldots \subseteq G_{k}=G
$$

such $G_{i} \triangleleft G$ and $G_{i+1} / G_{i} \subseteq Z\left(G / G_{i}\right)$ 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

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

We have

$$
\ldots \subseteq \Gamma_{1}(G) \subseteq \Gamma_{0}(G)=G
$$

24.11 Proposition. If $G$ is a group then

1) $\Gamma_{i}(G) \triangleleft G$ for all $i$
2) $\Gamma_{i}(G) / \Gamma_{i+1}(G) \subseteq Z\left(G / \Gamma_{i+1}(G)\right)$ 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.

Proof. Exercise.
24.15 Note. The properties of nilpotent group given in Theorem 24.14 are analogous to the first two properties of solvable groups from Theorem 23.6. The third part of that theorem (if $H, G / H$ are solvable then so is $G$ ) is not true for nilpotent groups. For example, take $G=G_{T}$ and $H=\left\{I, R_{1}, R_{2}\right\}$. Both $H$ and $G / H$ are nilpotent, but by (24.5) $G$ is not.
24.16 Proposition. If $G_{1}, \ldots, G_{k}$ are nilpotent groups then the direct product $G_{1} \times \cdots \times G_{k}$ is also nilpotent.

Proof. It will be enough to show that the statement holds for $k=2$, then the general case will follow by induction with respect to $k$. Notice for any groups $G_{1}, G_{2}$ we have $\Gamma_{i}\left(G_{1} \times G_{2}\right)=\Gamma_{i}\left(G_{1}\right) \times \Gamma_{i}\left(G_{2}\right)$. If $G_{1}$ and $G_{2}$ are nilpotent then by (24.13) there exists $n \geq 0$ such that $\Gamma_{n}\left(G_{1}\right)=\{e\}$ and $\Gamma_{n}\left(G_{2}\right)=\{e\}$. This implies that $\Gamma_{n}\left(G_{1} \times G_{2}\right)$ is trivial, and so using (24.13) again we obtain that $G_{1} \times G_{2}$ is nilpotent.
24.17 Corollary. If $p_{1}, \ldots, p_{k}$ 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 (24.16).
24.18 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.
24.19 Lemma. If $G$ is a finite group and $P$ is a Sylow $p$-subgroup of $G$ then

$$
N_{G}\left(N_{G}(P)\right)=N_{G}(P)
$$

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, $P \triangleleft N_{G}(P)$, so $P$ is the only Sylow $p$-subgroup of $G$.

Take $a \in N_{G}\left(N_{G}(P)\right)$. We will show that $a \in N_{G}(P)$. We have

$$
a P a^{-1} \subseteq a N_{G}(P) a^{-1}=N_{G}(P)
$$

As a consequence $a P a^{-1}$ is a Sylow $p$-subgroup of $N_{G}(P)$, and thus $a P a^{-1}=P$. By the definitions of normalizer this gives $a \in N_{G}(P)$.
24.20 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

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

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

$$
a h Z_{k}(G)=\left(a Z_{k}(G)\right)\left(h Z_{k}(G)\right)=\left(h Z_{k}(G)\right)\left(a Z_{k}(G)\right)=h a Z_{k}(G)
$$

Therefore $h a=a h h^{\prime}$ for some $h^{\prime} \in Z_{k}(G) \subseteq H$, and so $a^{-1} h a=h h^{\prime} \in H$. As a consequence $a^{-1} H a=H$, so $a^{-1} \in N_{G}(H)$, and so also $a \in N_{G}(H)$.

## Proof of Theorem 24.18.

$1) \Rightarrow 2$ ) 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 24.20 it is also a proper subgroup of $N_{G}\left(N_{G}(P)\right)$. On the other hand by Lemma 24.19 we have $N_{G}\left(N_{G}(P)\right)=N_{G}(P)$, so we obtain a contradiction.
2) $\Rightarrow$ 3) Exercise.
$3) \Rightarrow$ 1) Follows from Corollary 24.17.

## 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: $(a b) c=a(b c)$
3) addition is distributive with respect to multiplication:

$$
a(b+c)=a b+a c \quad(a+b) c=a c+b c
$$

The ring $R$ is commutative if $a b=b a$ for all $a, b \in R$.
The ring $R$ is a ring with identity if there is and element $1 \in R$ such that $a 1=1 a=a$ 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

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

3) If $R$ is a ring then

$$
R[x]=\left\{a_{0}+a_{1} x+\ldots+a_{n} x^{n} \mid a_{i} \in R, n \geq 0\right\}
$$

is the ring of polynomials with coefficients in $R$ and

$$
R[[x]]=\left\{a_{0}+a_{1} x+\ldots \mid a_{i} \in R\right\}
$$

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 $\operatorname{Hom}(G, G)$ of all homomorphisms $f: G \rightarrow G$ 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

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

addition in $R[G]$ :

$$
\sum_{g \in G} a_{g} g+\sum_{g \in G} b_{g} g=\sum_{g \in G}\left(a_{g}+b_{g}\right) g
$$

multiplication in $R[G]$ :

$$
\left(\sum_{g \in G} a_{g} g\right)\left(\sum_{g \in G} b_{g} g\right)=\sum_{g \in G}\left(\sum_{h h^{\prime}=g} a_{h} a_{h^{\prime}}\right) g
$$

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 $a b=0$ (resp. $b a=0$ ).

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

$$
a c=b c
$$

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 $a=b$.
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 $b a=1$ (resp. there exists $c \in R$ such that $c b=1$ ).

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 $b a=1=a c$ then

$$
b=b \cdot 1=b(a c)=(b a) c=1 \cdot c=c
$$

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

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

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

$$
\mathbb{H}:=\{a+b i+c j+d k \mid a, b, c, d \in \mathbb{R}\}
$$

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

$$
i^{2}=j^{2}=k^{2}=-1, \quad i j=-j i=k, \quad j k=-k j=i, \quad k i=-i k=j
$$

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

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

The inverse of an element $z=a+b i+c j+d k$ 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) $\mathbb{Z} / n \mathbb{Z}$ is a field.
2) $\mathbb{Z} / n \mathbb{Z}$ is an integral domain.
3) $n$ is a prime number.

Proof. Exercise.

## 26 Ring homomorphisms and ideals

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

$$
f: R \rightarrow S
$$

such that

1) $f(a+b)=f(a)+f(b)$
2) $f(a b)=f(a) f(b)$
26.2 Note. If $R, S$ are rings with identity then these conditions do not guarantee that $f\left(1_{R}\right)=1_{S}$.

Take e.g. rings with identity $R_{1}, R_{2}$ and define

$$
R_{1} \oplus R_{2}=\left\{\left(r_{1}, r_{2}\right) \mid r_{1} \in R_{1}, R_{2}\right\}
$$

with addition and multiplication defined coordinatewise. Then $R_{1} \oplus R_{2}$ is a ring with identity $\left(1_{R_{1}}, 1_{R_{2}}\right)$. The map

$$
f: R_{1} \rightarrow R_{1} \oplus R_{2}, \quad f\left(r_{1}\right)=\left(r_{1}, 0\right)
$$

is a ring homomorphism, but $f\left(1_{R_{1}}\right) \neq\left(1_{R_{1}}, 1_{R_{2}}\right)$.
26.3 Note. Rings and ring homomorphisms form a category $\mathcal{R i n g}$.
26.4 Proposition. A ring homomorphism $f: R \rightarrow S$ is an isomorphism of rings iff $f$ is a bijection.

Proof. Exercise.
26.5 Definition. If $f: R \rightarrow S$ is a ring homomorphism then

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

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

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 $a b \in I$. 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 $I \triangleleft R$.
26.9 Proposition. If $f: R \rightarrow S$ is a ring homomorphism then $\operatorname{Ker}(f)$ 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: $(a+I)(b+I)=a b+I$.
26.11 Note. If $I \triangleleft R$ then the map

$$
\pi: R \rightarrow R / I, \quad \pi(a)=a+I
$$

is a ring homomorphism. It is called the canonical epimorphism of $R$ onto $R / I$.
26.12 Theorem. If $f: R \rightarrow S$ is a homomorphism of rings then there is a unique homomorphism

$$
\bar{f}: R / \operatorname{Ker}(f) \rightarrow S
$$

such that the following diagram commutes:


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

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

Proof. Take the map $\bar{f}: R / \operatorname{Ker}(f) \rightarrow S$. 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.
26.14 Note. Let $I, J \triangleleft R$. Check:

1) $I \cap J \triangleleft R$
2) $I+J \triangleleft R$ 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.
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.

