Non-commutative algebra

Leandro Vendramin

Contents

Introduction

The notes correspond to the master course *Non-commutative Algebra* of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into twelve two-hour lectures.

Thanks go to Arjen Elbert Dujardin, Ilaria Colazzo, Robynn Corveleyn, Luca Descheemaeker, Wannes Malfait, Lucas Simons, and José Navarro Villegas.

This version was compiled on March 28, 2024 at 21:03.

Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel
E-mail address: Leandro.Vendramin@vub.be.

Lecture 1. 15/02/2024

§ 1.1. Solvable groups. A subgroup H of G is said to be **characteristic** if $f(H) \subseteq H$ for all $f \in \mathrm{Aut}(G)$. The center and the commutator subgroup are characteristic subgroups. Every characteristic subgroup is normal, as the maps $x \mapsto gxg^{-1}$ are automorphisms.

EXERCISE 1.1. Prove that if H is characteristic in K and K is normal in G, then H is normal in G.

For a group G and $x, y, z \in G$, conjugation will be considered as a left action of G on G and we will use the following notation: ${}^{x}y = xyx^{-1}$. The commutator between x and y will be written as

$$[x,y] = xyx^{-1}y^{-1} = ({}^{x}y)y^{-1}.$$

We will also use the following notation:

$$[x,y,z] = [x,[y,z]].$$

For subgroups H and K of G, let

$$[H,K] = \langle [h,k] : h \in H, k \in K \rangle.$$

Note that $[X,Y] = [Y,X]$. For subgroups X, Y and Z of G, we write

$$[X,Y,Z] = [X,[Y,Z]].$$

For a group G, let $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for $i \geq 0$. The **derived series** of G is the sequence

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

Each $G^{(i)}$ is a characteristic subgroup of G.

DEFINITION 1.2. We say that a group G is **solvable** if $G^{(n)} = \{1\}$ for some n.

EXAMPLE 1.3. Abelian groups are solvable.

EXAMPLE 1.4. The group $\mathbf{SL}_2(3)$ is solvable, as the derived series is

$$\mathbf{SL}_2(3) \supseteq Q_8 \supseteq C_4 \supseteq \{1\}.$$

EXAMPLE 1.5. Non-abelian simple groups cannot be solvable.

EXERCISE 1.6. Let G be a group. Prove the following statements:

1) A subgroup H of G is solvable, when G is solvable.

2) Let K be a normal subgroup of G. Then G is solvable if and only if K and G/K are solvable.

EXAMPLE 1.7. For $n \geq 5$ the group $\mathbb{A}_n$ is simple and non-abelian. Hence it is not solvable. It follows that $\mathbb{S}_n$ is not solvable for $n \geq 5$.

EXERCISE 1.8. Let p be a prime number. Prove that finite p-groups are solvable.

EXERCISE 1.9. Let p, q and r be prime numbers. Prove that groups of order $p^{\alpha}q$, p^2q^2 and pqr are solvable.

EXERCISE 1.10. Prove that groups of order < 60 are solvable.

THEOREM 1.11 (Burnside). *Let p be a prime number. If G is a finite group that has a conjugacy class with $p^k > 1$ elements, then G is not simple.*

The easiest way to prove Theorem 1.11 is using character theory.

THEOREM 1.12 (Burnside). *Let p and q be prime numbers. If G has order $p^a q^b$, then G is solvable.*

PROOF. If G is abelian, then it is solvable. Suppose now G is non-abelian. Let us assume that the theorem is not true. Let G be a group of minimal order $p^a q^b$ that is not solvable. Since $|G|$ is minimal, G is a non-abelian simple group. By the previous theorem, G has no conjugacy classes of size p^k nor conjugacy classes of size q^l with $k,l \geq 1$. The size of every conjugacy class of G is one or divisible by pq. Note that, since G is a non-abelian simple group, the center of G is trivial. Thus there is only one conjugacy class of size one. By the class equation,

$$|G| = 1 + \sum_{C:|C|>1} |C| \equiv 1 \bmod pq,$$

where the sum is taken over all conjugacy classes with more than one element, a contradiction. □

A recent generalization of Burnside's theorem is based on *word maps*. A word map of a group G is a map

$$G^k \to G, \quad (x_1,\ldots,x_k) \mapsto w(x_1,\ldots,x_k)$$

for some word $w(x_1,\ldots,x_k)$ of the free group F_k of rank k. Some word maps are surjective in certain families of groups. For example, Ore's conjecture is precisely the surjectivity of the word map $(x,y) \mapsto [x,y] = xyx^{-1}y^{-1}$ in every finite non-abelian simple group.

THEOREM 1.13 (Guralnick–Liebeck–O'Brien–Shalev–Tiep). *Let $a,b \geq 0$, p and q be prime numbers and $N = p^a q^b$. The map $(x,y) \mapsto x^N y^N$ is surjective in every non-abelian finite simple group.*

The proof appears in [**15**].

The theorem implies Burnside's theorem. Let G be a group of order $N = p^a q^b$. Assume that G is not solvable. Fix a composition series of G. There is a non-abelian factor S of order dividing N. Since S is simple non-abelian and $s^N = 1$ for all $s \in S$, it follows that the word map $(x,y) \mapsto x^N y^N$ has trivial image in S, a contradiction to the theorem.

THEOREM 1.14 (Feit–Thompson). *Groups of odd order are solvable.*

The proof of Feit–Thompson theorem is extremely hard. It occupies a full volume of the *Pacific Journal of Mathematics* [**10**]. A formal verification of the proof (based on the computer software Coq) was announced in [**14**]. This motivates a natural problem: To formally verify the classification of finite simple groups. Will mathematics move away from depending on just humans to verify proofs? Formal verification with computer-proof assistants could become the new standard for rigor in mathematics.

Back in the day, it was believed that if a certain divisibility conjecture is true, the proof of Feit–Thompson theorem could be simplified.

CONJECTURE 1.15 (Feit–Thompson). There are no prime numbers p and q such that $\frac{p^q-1}{p-1}$ divides $\frac{q^p-1}{q-1}$.

The conjecture remains open. However, now we know that proving the conjecture will not simplify further the proof of Feit–Thompson theorem.

In 2012, Le proved that the conjecture is true for $q = 3$, see [**25**].

In [**31**] Stephens proved that a certain stronger version of the conjecture does not hold, as the integers $\frac{p^q-1}{p-1}$ and $\frac{q^p-1}{q-1}$ could have common factors. In fact, if $p = 17$ and $q = 3313$, then

$$\gcd\left(\frac{p^q-1}{p-1}, \frac{q^p-1}{q-1}\right) = 112643.$$

Nowadays we can check this easily on almost every desktop computer:

```
gap> Gcd((17^3313-1)/16,(3313^17-1)/3312);
112643
```

No other counterexamples have been found of Stephen's stronger version of the conjecture.

Definition 1.16. Let p be a prime number. A p-group P is said to be **elementary abelian** if $x^p = 1$ for all $x \in P$.

Definition 1.17. A subgroup M of G is said to be **minimal normal** if $M \neq \{1\}$ (or $G = \{1\}$), M is normal in G and the only normal subgroup of G properly contained in M is $\{1\}$.

Example 1.18. If a normal subgroup M is minimal (with respect to the inclusion), then it is minimal and normal. However, the converse statement does not hold. For example, the subgroup of $\mathbb{A}_4$ generated by $(12)(34)$, $(13)(24)$ and $(14)(23)$ is minimal normal in $\mathbb{A}_4$ but it is not minimal.

Exercise 1.19. Prove that every finite group contains a minimal normal subgroup.

Example 1.20. Let $G = \mathbb{D}_6 = \langle r, s : r^6 = s^2 = 1, srs = r^{-1}\rangle$ the dihedral group of twelve elements. The subgroups $S = \langle r^2\rangle$ and $T = \langle r^3\rangle$ are (the only) minimal normal in G.

Example 1.21. Let $G = \mathbf{SL}_2(3)$. The only minimal normal subgroup of G is its center $Z(\mathbf{SL}_2(3)) \simeq C_2$.

The following lemma will be very useful later.

Lemma 1.22. *Let M be a minimal normal subgroup of G. If M is solvable and finite, then M is an elementary abelian p-group for some prime number p.*

Proof. Since M is solvable, $[M,M] \subsetneq M$. Moreover, $[M,M]$ is normal in G, as $[M,M]$ is characterisitic in M and M is normal in G. Since M is minimal normal, $[M,M] = \{1\}$. Hence M is abelian.

Since M is finite, there is a prime number p such that $\{1\} \neq P = \{x \in M : x^p = 1\} \subseteq M$. Since P is characteristic in M, P is normal in G. By minimality, $P = M$. □

Theorem 1.23. *Let G be a finite non-trivial solvable group. Then every maximal subgroup of G has index p^α for some prime number p.*

Proof. We proceed by induction on $|G|$. If $|G|$ is a prime power, the claim is clear. Assume that $|G| \geq 6$ and let M be a maximal subgroup of G. Let N be a minimal normal subgroup of G and $\pi\colon G \to G/N$ the canonical map. If $N = G$, then $N = G$ is a p-group and we are done. Assume then that $N \neq G$. Since $M \subseteq NM \subseteq G$, either $M = NM$ or $NM = G$ (by the maximality of M). If $M = NM \supseteq N$, then $\pi(M)$ is a maximal subgroup of $\pi(G) = G/N$. Hence

$$(G : M) = (\pi(G) : \pi(M))$$

is a prime power by the inductive hypothesis. If $NM = G$, then

$$(G : M) = \frac{|G|}{|M|} = \frac{|NM|}{|M|} = \frac{|N|}{|N \cap M|}$$

is a prime power, because N is a p-group by the previous lemma. □

EXERCISE 1.24. Let G be a finite non-trivial solvable group. Prove that there exists a prime number p such that G contains a minimal normal p-subgroup.

EXAMPLE 1.25. Let $G = \mathbb{S}_4$. The 2-subgroup

$$K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$$

is minimal normal. Note that G does not have minimal normal 3-subgroups.

THEOREM 1.26. *Let G be a finite non-trivial group. Then G is solvable if and only if every non-trivial quotient of G contains an abelian non-trivial normal subgroup.*

PROOF. Every quotient of G is solvable and therefore contains an abelian minimal normal subgroup. To prove the converse we proceed by induction on $|G|$. Let N be a normal abelian subgroup of G. If $N = G$, then G is solvable (because it is abelian). If $N \neq G$, then $|G/N| < |G|$. Since every quotient of G/N is a quotient of G, the group G/N satisfies the assumptions of the theorem. Hence G/N is solvable by the inductive hypothesis. Now N and G/N are solvable, so is G. □

EXERCISE 1.27. Let G be a group. Prove that G is solvable if and only if there is a sequence

$$\{1\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = G$$

of normal subgroups such that every quotient N_i/N_{i-1} is abelian.

§ 1.2. Hall's theorem. We start with an extremely simple and useful tool.

LEMMA 1.28 (Frattini's argument). *Let G be a finite group and K be a normal subgroup of G. If $P \in \mathrm{Syl}_p(K)$ for some prime number p, then $G = KN_G(P)$.*

PROOF. Let $g \in G$. Since $gPg^{-1} \subseteq gKg^{-1} = K$, because K is normal in G, and $gPg^{-1} \in \mathrm{Syl}_p(K)$, there exists $k \in K$ such that $kPk^{-1} = gPg^{-1}$. Hence $k^{-1}g \in N_G(P)$, as $P = (k^{-1}g)P(k^{-1}g)^{-1}$. Therefore $g = k(k^{-1}g) \in KN_G(P)$. □

THEOREM 1.29 (Hall). *Let G be a finite group such that every maximal subgroup of G has a prime or a prime-square index. Then G is solvable.*

PROOF. We proceed by induction on $|G|$. Let p be the largest prime divisor of $|G|$. Let $S \in \mathrm{Syl}_p(G)$ and $N = N_G(S)$.

If $N = G$, then S is normal in G. Since every maximal subgroup of G/S has prime or a prime-square index, G/S is solvable by the inductive hypothesis. Since S is a p-group, it is solvable. Therefore G is solvable.

Assume now that $N \neq G$. Let H be a maximal subgroup of G containing N. Then

$$N = N_H(S) = N_G(S),$$

the number of Sylow p-subgroups of G is $(G:N) \equiv 1 \mod p$ and the number of Sylow p-subgroups of H is $(H:N) \equiv 1 \mod p$ by the third Sylow's theorem. So,

$$\underbrace{(G:N)}_{\equiv 1 \mod p} = (G:H)\underbrace{(H:N)}_{\equiv 1 \mod p},$$

implies that also $(G:H) \equiv 1 \mod p$. By assumption, there exists a prime number q such that $(G:H) \in \{q, q^2\}$. Since q divides $|G|$, it follows that $q < p$. If $(G:H) = q$, then p divides $q-1$ and therefore $p \leq q-1 < p$, a contradiction. Thus $q^2 = (G:H) \equiv 1 \mod p$. From this it follows that $q \equiv -1 \mod p$ and hence $q = 2$ and $p = q+1 = 3$.

Therefore G has order $2^\alpha 3^\beta$. If we apply Burnside's theorem, we are done. Instead, we will finish the proof with an elementary argument. Let K be a minimal normal subgroup of G. By Frattini's argument (Lemma 1.28), $G = KN = KH$. Since H is maximal,

$$(K : K \cap H) = (G:H) = 4,$$

as $(G:H) = |G|/|H| = |KH|/|H| = |K|/|K \cap H|$. Since $(K : K \cap H) = 4$, letting K act on $K/K \cap H$ by left multiplication, there exists a non-trivial group homomorphism $\rho\colon K \to \mathbb{S}_4$. Since $[K,K]$ is characteristic in K and K is normal in G, $[K,K] \subseteq K$ is normal in G. Since K is minimal normal in G, there are two possible cases: either $[K,K] = \{1\}$ or $[K,K] = K$. If $[K,K] = K$, since $\mathbb{S}_4$ is solvable, $\rho(K)$ is solvable. Then

$$\rho(K) = \rho([K,K]) = [\rho(K), \rho(K)],$$

a contradiction. Therefore $[K,K] = \{1\}$ and K is solvable (as it is abelian). □

Lecture 2. 22/02/2024

§ 2.1. Wielandt's solvability theorem.

LEMMA 2.1. *Let G be a finite group and H and K be subgroups of G of coprime indices. Then $G = HK$ and $(H : H \cap K) = (G : K)$.*

PROOF. Let $D = H \cap K$. Since

$$(G : D) = \frac{|G|}{|H \cap K|} = (G : H)(H : H \cap K),$$

$(G : H)$ divides $(G : D)$. Similarly, $(G : K)$ divides $(G : D)$. Since $(G : H)$ and $(G : K)$ are coprime, $(G : H)(G : K)$ divides $(G : D)$. In particular,

$$\frac{|G|}{|H|}\frac{|G|}{|K|} = (G : H)(G : K) \leq (G : D) = \frac{|G|}{|H \cap K|}$$

and hence $|G| = |HK|$. Since

$$|G| = |HK| = |H||K|/|H \cap K|,$$

we conclude that $(G : K) = (H : H \cap K)$. □

DEFINITION 2.2. Let G be a group and H be a subgroup of G. The **normal closure** H^G of H in G is the subgroup $H^G = \langle xHx^{-1} : x \in G \rangle$.

EXERCISE 2.3. Let G be a group and H a subgroup of G. Prove that H^G is normal in G and that H^G is the smallest normal subgroup of G containing H.

EXAMPLE 2.4. Let $G = \mathbb{A}_4$ and $H = \{\mathrm{id}, (12)(34)\}$. The normal closure of H in G is

$$H^G = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2.$$

THEOREM 2.5 (Wielandt's solvability theorem). *Let G be a finite group and H, K and L be subgroups of G with pairwise coprime indices. If H, K and L are solvable, then G is solvable.*

PROOF. Let G be a minimal counterexample. Then $G \neq \{1\}$. There are two cases to consider. Assume first that $H = \{1\}$. Then $|G| = (G : H)$ is coprime with $(G : K)$ and thus $G = K$ is solvable. Assume now that $H \neq \{1\}$. Let M be a minimal normal subgroup of H. By Lemma 1.22, M is a p-group for some prime number p. Without loss of generality, we may assume that p does not divide $(G : K)$ (otherwise, if p divides $(G : K)$, then p does not divide $(G : L)$ and we just need to change K by L). There exists $P \in \mathrm{Syl}_p(G)$ such that $P \subseteq K$. Sylow subgroups are conjugate, so there exists $g \in G$ such that $M \subseteq gKg^{-1}$. Since $(G : gKg^{-1}) = (G : K)$ is coprime with $(G : H)$, Lemma 2.1 implies that $G = (gKg^{-1})H$.

We claim that all conjugates of M are in gKg^{-1}. If $x \in G$, write $x = uv$ some some $u \in gKg^{-1}$ and $v \in H$. Since M is normal in H,

$$xMx^{-1} = (uv)M(uv)^{-1} = uMu^{-1} \subseteq gKg^{-1}.$$

Let $N = M^G$ be the normal closure of M in G. Then $\{1\} \neq N \subseteq gKg^{-1}$ is solvable, as gKg^{-1} is solvable. We claim that G/N is solvable. Let $\pi\colon G \to G/(M^G)$ be the canonical map. Since H, K and L are solvable, the subgroups $\pi(H)$, $\pi(K)$ and $\pi(L)$ of $\pi(G)$ are solvable. By the correspondence theorem, $\pi(H)$, $\pi(K)$ and $\pi(L)$ have pairwise coprime indices. Moreover, $\pi(G)$ is solvable, as $|\pi(G)| < |G|$. Hence G is solvable. □

§ 2.2. Hall's theorem.

DEFINITION 2.6. Let G be a finite group of order $p^\alpha m$, where p is a prime number such that $\gcd(p,m)=1$. A subgroup H of G is said to be a **p-complement** if $|H|=m$.

EXAMPLE 2.7. Let $G=\mathbb{S}_3$. Then $H=\langle(123)\rangle$ is a 2-complement and $K=\langle(12)\rangle$ is a 3-complement.

THEOREM 2.8 (Hall). *Let G be a finite group that admits a p-complement for every prime divisor p of $|G|$. Then G is solvable.*

PROOF. Let $|G|=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ with $p_1<\cdots<p_k$ prime numbers. We proceed by induction on k. If $k=1$, then the claim holds, as G is a p-group. If $k=2$, the result holds by Burnside's theorem. Assume now that $k\geq 3$. For $j\in\{1,2,3\}$, let H_j be a p_j-complement in G. Since $|H_j|=|G|/p_j^{\alpha_j}$, the subgroups H_j have pairwise coprime indices.

We claim that H_1 is solvable. Note that $|H_1|=p_2^{\alpha_2}\cdots p_k^{\alpha_k}$. Let p be a prime number dividing $|H_1|$ and Q be a p-complement in G. Since $(G:H_1)$ and $(G:Q)$ are coprime, Lemma 2.1 implies that

$$(H_1:H_1\cap Q)=(G:Q).$$

Then $H_1\cap Q$ is a p-complement in H_1. Therefore H_1 is solvable by the inductive hypothesis. Similarly, both H_2 and H_3 are solvable.

Since H_1, H_2 and H_3 are solvable of pairwise coprime indices, the theorem follows from Wielandt's theorem. □

§ 2.3. Nilpotent groups.

EXERCISE 2.9 (The Hall–Witt identity). Let G be a group and $x,y,z\in G$. Prove that

$$\left({}^{y}[x,y^{-1},z]\right)\left({}^{z}[y,z^{-1},x]\right)\left({}^{x}[z,x^{-1},y]\right)=1. \tag{2.1}$$

If G is a group and $[G,G]$ is central in G, then the Hall-Witt identity becomes Jacobi's identity.

LEMMA 2.10 (Hall's three subgroups lemma). *Let X, Y and Z be subgroups of G such that $[X,Y,Z]=[Y,Z,X]=\{1\}$. Then $[Z,X,Y]=\{1\}$.*

PROOF. Since $[x,y]\in C_G(z)$ implies $[X,Y]\subseteq C_G(Z)$, it is enough to prove that $[z,x^{-1},y]=1$ for all $x\in X$, $y\in Y$ and $z\in Z$. Since $[y^{-1},z]\in[Y,Z]$, $[x,y^{-1},z]\in[X,Y,Z]=\{1\}$. Thus ${}^{y}[x,y^{-1},z]=1$. Similarly, ${}^{z}[y,z^{-1},x]=1$. Using the Hall–Witt identity, we conclude that $[z,x^{-1},y]=1$. □

EXERCISE 2.11. Let N be a normal subgroup of G and X, Y and Z be subgroups of G. If $[X,Y,Z]\subseteq N$ and $[Y,Z,X]\subseteq N$, then $[Z,X,Y]\subseteq N$.

DEFINITION 2.12. Let G be a group. The **lower central series** is the sequence $\gamma_k(G)$ of subgroups defined inductively as

$$\gamma_1(G)=G,\quad \gamma_{i+1}(G)=[G,\gamma_i(G)]\quad i\geq 1.$$

DEFINITION 2.13. A group G is said to be **nilpotent** if there exists a positive integer c such that $\gamma_{c+1}(G)=\{1\}$. The smallest c with $\gamma_{c+1}(G)=\{1\}$ is the **nilpotency class** of G.

EXERCISE 2.14. Prove that every nilpotent group is solvable.

A group is nilpotent of nilpotency class one if and only if it is abelian.

EXAMPLE 2.15. The group $\mathbb{S}_3$ is solvable, as $\mathbb{S}_3 \supseteq \mathbb{A}_3 \supseteq \{1\}$ is a composition series with abelian factors. However, $\mathbb{S}_3$ is not nilpotent, as

$$\gamma_1(\mathbb{S}_3) = \mathbb{A}_3, \quad \gamma_2(\mathbb{S}_3) = [\mathbb{A}_3, \mathbb{S}_3] = \mathbb{A}_3,$$

and therefore $\gamma_i(\mathbb{S}_3) \neq \{1\}$ for all $i \geq 1$.

EXAMPLE 2.16. The group $G = \mathbb{A}_4$ is not nilpotent, as

$$\gamma_1(G) = G, \quad \gamma_j(G) = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2$$

for all $j \geq 2$. We can do this with the computer:

```
gap> IsNilpotent(AlternatingGroup(4));
false
```

Let us do the calculation of the lower central series with the computer:

```
gap> List(LowerCentralSeries(AlternatingGroup(4)),\
StructureDescription);
[ "A4", "C2 x C2" ]
```

Here is an alternative:

```
gap> G := AlternatingGroup(4);;
gap> gamma_1 := G;;
gap> gamma_2 := DerivedSubgroup(G);;
gap> gamma_3 := CommutatorSubgroup(gamma_2,G);;
gap> StructureDescription(gamma_1);
"A4"
gap> StructureDescription(gamma_2);
"C2 x C2"
gap> StructureDescription(gamma_3);
"C2 x C2"
```

EXERCISE 2.17. Let G be a group. Prove the following statements:

1) Each $\gamma_i(G)$ is a characteristic subgroup of G.
2) $\gamma_i(G) \supseteq \gamma_{i+1}(G)$ for all $i \geq 1$.
3) If $f\colon G \to H$ is a surjective group homomorphism, then $f(\gamma_i(G)) = \gamma_i(H)$ for all $i \geq 1$.

EXERCISE 2.18. Prove that if H and K are nilpotent groups, then $H \times K$ is nilpotent.

EXERCISE 2.19. Let G be a nilpotent group. Prove the following statements:

1) Subgroups of G are nilpotent.
2) If $f\colon G \to H$ is a surjective homomorphism, then H is nilpotent.

EXERCISE 2.20. True or false? If G is a nilpotent group and N is normal subgroup of G such that N and G/N are nilpotent, then G is nilpotent.

PROPOSITION 2.21. *Finite p-groups are nilpotent.*

PROOF. We proceed by induction on $|G|$. The case $G = \{1\}$ is trivial. Assume the result holds for p-groups of order $< |G|$. Since G is a p-group, $Z(G) \neq \{1\}$. By the inductive hypothesis, $G/Z(G)$ is nilpotent. There exists c such that $\gamma_{c+1}(G/Z(G)) = \{1\}$.

Let $\pi\colon G \to G/Z(G)$ be the canonical map. By Exercise 2.17,

$$\pi(\gamma_{c+1}(G)) = \gamma_{c+1}(G/Z(G)) = \{1\}.$$

Then $\gamma_{c+1}(G) \subseteq \ker \pi = Z(G)$. Hence G is nilpotent, as

$$\gamma_{c+2}(G) = [G, \gamma_{c+1}(G)] = [G, Z(G)] = \{1\}. \qquad \square$$

THEOREM 2.22. *If G is a group, then $[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G)$ for all $i, j \geq 1$.*

PROOF. We proceed by induction on i. The case $i = 1$ is trivial, as $[G, \gamma_j(G)] = \gamma_{j+1}(G)$ by definition. Assume that the result holds for some $i \geq 1$ and all $j \geq 1$.

First note that

$$[G, \gamma_i(G), \gamma_j(G)] \subseteq [G, \gamma_{i+j}(G)] = \gamma_{i+j+1}(G)$$

by the inductive hypothesis. Moreover, by the inductive hypothesis,

$$[\gamma_i(G), \gamma_j(G), G] = [\gamma_i(G), G, \gamma_j(G)] = [\gamma_i(G), \gamma_{j+1}(G)] \subseteq \gamma_{i+j+1}(G)$$

By using Exercise 2.11 with $X = G$, $Y = \gamma_i(G)$ and $Z = \gamma_j(G)$, we get that

$$[\gamma_j(G), G, \gamma_i(G)] \subseteq \gamma_{i+j+1}(G).$$

Hence

$$[\gamma_{i+1}(G), \gamma_j(G)] = [\gamma_j(G), \gamma_{i+1}(G)] = [\gamma_j(G), G, \gamma_i(G)] \subseteq \gamma_{i+j+1}(G). \qquad \square$$

We may have to consider commutators with n copies of the group that are not necessarily associated on the right. For example, if $n = 3$, we might have something like $[G, G, G] = [G, [G, G]]$ or $[[G, G], G]$. These expressions will be called commutators of **weight** three.

COROLLARY 2.23. *In a group G, every weight n commutator is contained in $\gamma_n(G)$.*

PROOF. We proceed by induction on n. The case $n = 1$ is trivial. Assume that $n \geq 1$ and the result holds for all $j \leq n$. An arbitrary commutator of weight $n+1$ is of the form $[A, B]$, where A is a commutator of weight k, B is a commutator of weight l and $n + 1 = k + l$. Since $k \leq n$ and $l \leq n$, the inductive hypothesis implies that $A \subseteq \gamma_k(G)$ and $B \subseteq \gamma_l(G)$. Hence $[A, B] \subseteq [\gamma_k(G), \gamma_l(G)] \subseteq \gamma_{k+l}(G)$ by the previous theorem. $\square$

EXERCISE 2.24. Let G be a group. Prove that $G^{(k)} \subseteq \gamma_{2^k}(G)$ for all $k \geq 1$.

EXERCISE 2.25. Let G be a nilpotent group of class m. Prove that the derived length (i.e. the length of the derived series) of G is $\leq 1 + \log_2 m$.

The following lemma is important. It states that nilpotent groups satisfy the **normalizer condition**.

LEMMA 2.26 (normalizer condition). *Let G be a nilpotent group. If H is a proper subgroup of G, then $H \subsetneq N_G(H)$.*

PROOF. There exists c such that $G = \gamma_1(G) \supseteq \cdots \supseteq \gamma_{c+1}(G) = \{1\}$. Since $\{1\} = \gamma_{c+1}(G) \subseteq H$ and $\gamma_1(G) \not\subseteq H$, let k be the smallest positive integer such that $\gamma_k(G) \subseteq H$. Since

$$[H, \gamma_{k-1}(G)] \subseteq [G, \gamma_{k-1}(G)] = \gamma_k(G) \subseteq H,$$

we obtain that $xHx^{-1} \subseteq H$ for all $x \in \gamma_{k-1}(G)$, that is $\gamma_{k-1}(G) \subseteq N_G(H)$. If $N_G(H) = H$, then $\gamma_{k-1}(G) \subseteq H$, a contradiction to the minimality of k. □

For a group G, we define the sequence $\zeta_0(G), \zeta_1(G), \ldots$ recursively as follows:

$$\zeta_0(G) = \{1\}, \quad \zeta_{i+1}(G) = \{g \in G : [x,g] \in \zeta_i(G) \text{ for all } x \in G\}, \quad i \geq 0.$$

For example, $\zeta_1(G) = Z(G)$.

LEMMA 2.27. *Let G be a group. For every $i \geq 0$, the set $\zeta_i(G)$ is a normal subgroup of G.*

PROOF. We proceed by induction on i. The case $i = 0$ is trivial, as $\zeta_0(G) = \{1\}$. Assume the result holds for some i. We claim that $\zeta_{i+1}(G)$ is normal subgroup of G. Let $g, h \in \zeta_{i+1}(G)$ and $x \in G$. By the inductive hypothesis,

$$[x, g^{-1}] = (xg^{-1})[x^{-1}, g](xg^{-1})^{-1} \in \zeta_i(G)(xg^{-1})^{-1} = \zeta_i(G),$$
$$[x, gh] = [x,h][hxh^{-1}, g] \in \zeta_i(G).$$

Since $1 \in \zeta_{i+1}(G)$, we conclude that each $\zeta_i(G)$ is a subgroup of G. Moreover, since

$$[xgx^{-1}, y] = x[g, x^{-1}yx]x^{-1} \in \zeta_i(G)$$

for all $y \in G$, we obtain that $xgx^{-1} \in \zeta_{i+1}(G)$. □

DEFINITION 2.28. Let G be a group. The **ascending central series** of G is the sequence

$$\{1\} = \zeta_0(G) \subseteq \zeta_1(G) \subseteq \zeta_2(G) \subseteq \cdots$$

DEFINITION 2.29. A group G is said to be **perfect** if $[G, G] = G$.

THEOREM 2.30 (Grün). *If G is a perfect group, then $Z(G/Z(G)) = \{1\}$.*

PROOF. By definition, $[G, \zeta_2(G)] \subseteq Z(G)$ and $[\zeta_2(G), G] \subseteq Z(G)$. Then

$$[G, G, \zeta_2(G)] = [G, \zeta_2(G), G] = \{1\}.$$

By using the three subgroups lemma with $X = Y = G$ and $Z = \zeta_2(G)$,

$$[\zeta_2(G), G] = [\zeta_2(G), [G, G]] = [\zeta_2(G), G, G] = \{1\}.$$

Thus $\zeta_2(G) \subseteq Z(G)$.

We aim to prove that $Z(G/Z(G))$ is trivial. Let $\pi\colon G \to G/Z(G)$ be the canonical map and $g \in G$ be such that $\pi(g)$ is central. Since

$$1 = [\pi(x), \pi(g)] = \pi([x,g])$$

for all $x \in G$, $[x,g] \in Z(G) = \zeta_1(G)$ for all $x \in G$. Hence $g \in \zeta_2(G) \subseteq Z(G)$. □

§ 2.4. Berkovich's theorem. We start with an exercise on the **normal core** of a subgroup.

EXERCISE 2.31. Let G be a group and A be a subgroup of G. Prove that

$$\mathrm{Core}_G(A) = \bigcap_{x\in G} xAx^{-1}$$

is the largest normal subgroup of G contained in A.

THEOREM 2.32 (Berkovich). *Let G be a finite solvable group and H be a proper subgroup of G with the smallest possible index. Then H is normal in G.*

PROOF. Note that H is a maximal subgroup. Let $C = \mathrm{Core}_G(H)$. There are two cases to consider.

Assume first that $C \neq \{1\}$. Let $\pi\colon G \to G/C$ be the canonical map. By the inductive hypothesis, $\pi(H)$ is normal in $\pi(G) = G/C$, as by the correspondence theorem,

$$(\pi(G) : \pi(H)) = (G : H)$$

is the smallest possible index in G/C. Thus H is normal in G again by the correspondence theorem.

Assume now that $C = \{1\}$. Let N be a minimal normal subgroup of G. Since N is abelian, $N \cap H$ is normal in N. Moreover, since N is normal in G, $N \cap H$ is normal in H. Thus $N \cap H$ is a normal subgroup of NH.

We claim that $N \not\subseteq H$. If $N \subseteq H$, then, for every $x \in G$,

$$N = xNx{-}1 \subseteq xHx^{-1}.$$

Therefore

$$N \subseteq \bigcap_{x\in G} xHx^{-1} = \mathrm{Core}_G(H) = \{1\},$$

a contradiction.

Since H is maximal, either $NH = G$ or $NH = H$. If $NH = H$, then $N \subseteq NH = H$, a contradiction. Hence $NH = G$. Thus $N \cap H$ is a normal subgroup of $NH = G$. The minimality of N implies then that $N \cap H = \{1\}$ and therefore

$$|N||H| = \frac{|N||H|}{|N \cap H|} = |G|.$$

This implies that $|N| = (G : H)$.

Let H act on N by conjugation. By the fundamental counting principle,

$$|H \cdot x| = (H : H_x)$$

for all $x \in N$. Since $H \cdot 1 = \{1\}$, every orbit has at most $|N| - 1$ elements, that is

$$(H : H_x) = |H \cdot x| \leq |N| - 1.$$

for all $x \in N$.

Since N is a normal subgroup of G, the set NH_x is a subgroup of G. Moreover,

$$N \cap H_x \subseteq N \cap H = \{1\}.$$

Thus

$$(G : NH_x) = \frac{|G|}{|NH_x|} = \frac{|G|}{|N||H_x|} = \frac{|N||H|}{|N||H_x|} = (H : H_x) \leq |N| - 1 = (G : H) - 1,$$

a contradiction. □

The solution of the following exercise is implicit in the proof of Berkovich's theorem.

EXERCISE 2.33. Let G be a finite solvable group and H a subgroup of G. Assume that H is contained in maximal subgroup M such that $\mathrm{Core}_G(M) = \{1\}$. Prove that G has a subgroup with index equal to $(M : H)$.

§ 2.5. *Carter subgroups.

DEFINITION 2.34. Let G be a finite group. A **Carter subgroup** of G is a nilpotent subgroup C of G such that $C = N_G(C)$.

THEOREM 2.35 (Carter). *Every finite solvable group has a Carter subgroup. Moreover, every two Carter subgroups are conjugate.*

PROOF. See [**5**]. □

Note that solvability is a needed assumption. For example, the group $\mathbb{A}_5$ does not have Carter subgroups.

EXERCISE 2.36. Let G be a finite solvable group and C be a Carter subgroup. Let N be a normal subgroup of G such that G/N is nilpotent. Prove that $NC = G$.

Vdovin showed that even if a finite group is not solvable then any two Carter subgroups are conjugate. The proof is difficult and uses the classification of finite simple groups.

Lecture 3. 29/02/2024

Let G be a group and K be a subgroup of G. We say that K **normalizes** H if $K \subseteq N_G(H)$. We say that K **centralizes** H if $K \subseteq C_G(H)$, that is if and only if $[H,K] = \{1\}$.

EXERCISE 3.1. Let K and H be subgroups of G such that $K \subseteq H$ and K is normal in G. Prove that $[H,G] \subseteq K$ if and only if $H/K \subseteq Z(G/K)$.

LEMMA 3.2. *Let G be a group. There exists an integer c such that $\zeta_c(G) = G$ if and only if $\gamma_{c+1}(G) = \{1\}$. In this case,*

$$\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$$

for all $i \in \{0,1,\ldots,c\}$.

PROOF. Assume first that $\zeta_c(G) = G$. To prove that $\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$ holds for all i, we proceed by induction. The case $i = 0$ is trivial. So assume that the result holds for some $i \geq 0$. If $g \in \gamma_{i+2}(G) = [G, \gamma_{i+1}(G)]$, then

$$g = \prod_{k=1}^{N} [x_k, g_k],$$

for some $g_1, \ldots, g_N \in \gamma_{i+1}(G)$ and $x_1, \ldots, x_N \in G$. By the inductive hypothesis,

$$g_k \in \gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$$

for all k. Hence $[x_k, g_k] \in \zeta_{c-i-1}(G)$ for all k. Therefore $g \in \zeta_{c-(i+1)}(G)$.

We now assume that $\gamma_{c+1}(G) = \{1\}$. We aim to prove that $\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$ holds for all i. We proceed by backward induction on i. The case $i = c$ is trivial. So assume the result holds for some $i+1 \leq c$. Let $g \in \gamma_i(G)$. By the inductive hypothesis,

$$[x,g] \in [G, \gamma_i(G)] = \gamma_{i+1}(G) \subseteq \zeta_{c-i}(G).$$

Thus $g \in \zeta_{c-i+1}(G)$ by definition. □

EXAMPLE 3.3. Let $G = \mathbb{S}_3$. Then $\zeta_j(G) = \{1\}$ for all $j \geq 0$:

```
gap> UpperCentralSeries(SymmetricGroup(3));
[ Group(()) ]
```

DEFINITION 3.4. Let G be a group. A **central series** for G is a sequence

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

of normal subgroups of G such that for each $i \in \{1,\ldots,n\}$, $\pi_i(G_{i-1})$ is a subgroup of $Z(G/G_i)$, where $\pi_i \colon G \to G/G_i$ is the canonical map.

LEMMA 3.5. *Let $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ be a central series of a group G. Then $\gamma_{i+1}(G) \subseteq G_i$ for all i.*

PROOF. We proceed by induction on i. The case $i = 0$ is trivial. So assume the result holds for some $i \geq 0$. Let $\pi_i \colon G \to G/G_i$ be the canonical map. Then

$$\gamma_{i+1}(G) = [G, \gamma_i(G)] \subseteq [G, G_{i-1}].$$

Since $\pi_i(G_{i-1}) \subseteq Z(G/G_i)$,

$$\pi_i([G, G_{i-1}]) = [\pi_i(G), \pi_i(G_{i-1})] = \{1\}.$$

Hence $\gamma_{i+1}(G) \subseteq [G, G_{i-1}] \subseteq G_i$. □

THEOREM 3.6. *A group is nilpotent if and only if it admits a central series.*

PROOF. Let G be a group. If G is nilpotent, then the $\gamma_j(G)$ form a central series of G. Conversely, if $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ is a central series of G, then, by the previous lemma,

$$\gamma_{n+1}(G) \subseteq G_n = \{1\}.$$

Hence G is nilpotent. □

EXERCISE 3.7. Let G be a group. Prove that if K is a subgroup of $Z(G)$ such that G/K is nilpotent, then G is nilpotent.

§ 3.1. Hirsch's theorem.

THEOREM 3.8 (Hirsch). *Let G be a non-trivial nilpotent group. If H is a non-trivial normal subgroup of G, then $H \cap Z(G) \neq \{1\}$. In particular, $Z(G) \neq \{1\}$.*

PROOF. Since $\zeta_0(G) = \{1\}$ and there exists an integer c such that $\zeta_c(G) = G$, there exists

$$m = \min\{k : H \cap \zeta_k(G) \neq \{1\}\}.$$

Since H is normal in G,

$$[G, H \cap \zeta_m(G)] \subseteq H \cap [G, \zeta_m(G)] \subseteq H \cap \zeta_{m-1}(G) = \{1\}.$$

Therefore $\{1\} \neq H \cap \zeta_m(G) \subseteq H \cap Z(G)$. If $H = G$, then $Z(G) \neq \{1\}$. □

EXERCISE 3.9. Let G be a nilpotent group and M be a minimal normal subgroup of G. Prove that $M \subseteq Z(G)$.

DEFINITION 3.10. Let G be a group. A subgroup M is said to be **maximal normal** in G if $M \neq G$ and M is the only proper normal subgroup of G containing M.

COROLLARY 3.11. *Let G be a non-abelian nilpotent group, and A be a maximal normal and abelian subgroup of G. Then $A = C_G(A)$.*

PROOF. Since A is abelian, $A \subseteq C_G(A)$. Assume that $A \neq C_G(A)$. The centralizer $C_G(A)$ is normal in G, since A is normal in G and

$$gC_G(A)g^{-1} = C_G(gAg^{-1}) = C_G(A)$$

for all $g \in G$. Let $\pi\colon G \to G/A$ be the canonical map. Then $\pi(C_G(A))$ is a non-trivial normal subgroup of $\pi(G)$. Since G is nilpotent, $\pi(G)$ is nilpotent. By Hirsch's theorem,

$$\pi(C_G(A)) \cap Z(\pi(G)) \neq \{1\}.$$

Let $x \in C_G(A) \setminus A$ be such that $\pi(x)$ is central in $\pi(G)$. Then $\langle A, x\rangle$ is abelian, as $x \in C_G(A)$. Moreover, $\langle A, x\rangle$ is normal in G, as A is normal in G and $gxg^{-1}x^{-1} \in A$ for all $g \in G$ (because $\pi(x)$ is central). Hence $gxg^{-1} \in \langle A, x\rangle$ and therefore $A \subsetneq \langle A, x\rangle \subsetneq G$, a contradiction. □

THEOREM 3.12. *Let G be a nilpotent group. The following statements hold:*

1) *Every minimal normal subgroup of G has prime order and is central.*
2) *Every maximal subgroup of G is normal of prime index and contains $[G, G]$.*

PROOF.

1) Let N be a minimal normal subgroup of G. Since $N \cap Z(G) \neq \{1\}$ by Hirsch's theorem, $N \cap Z(G)$ is a normal subgroup of G contained in N. Then $N = N \cap Z(G) \subseteq Z(G)$ by the minimality of N. In particular, N is abelian. Since every subgroup of N is normal in G, N is simple. Hence $N \simeq C_p$ for some prime number p.

2) If M is a maximal subgroup, then M is normal in G by the normalizer condition (Lemma 2.26). By the maximality of M, the quotient G/M contains no proper non-trivial subgroups. Thus $G/M \simeq C_p$ for some prime p. Since G/M is abelian, $[G,G] \subseteq M$. □

The previous theorem does not prove the existence of maximal subgroups. For example, $\mathbb{Q}$ is a nilpotent group (as it is abelian) that contains no maximal subgroups.

PROPOSITION 3.13. *Let G be a nilpotent group and H be a subgroup with $(G:H) = n$. If $g \in G$, then $g^n \in H$.*

PROOF. We proceed by induction on n. The case $n = 1$ is trivial. The case $n = 2$ follows from the normality of H. So assume the result holds for all groups of index $< n$. Let H be a subgroup of G such that $(G:H) = n$. Let $H_0 = H$ and $H_{i+1} = N_G(H_i)$ for all $i \geq 0$. By definition, H_i is normal in H_{i+1}. Since G is nilpotent, $H_i \neq G$ implies that $H_i \subsetneq H_{i+1}$ by the normalizer condition. Since $(G:H)$ is finite, there exists k such that $H_k = G$. Since $(H_j : H_{j-1}) < n$ for all j, the inductive hypothesis implies that $x^{(H_j:H_{j-1})} \in H_{j-1}$ for all $x \in H_j$ and all j. Hence

$$g^{(G:H)} = g^{(H_k:H_{k-1})(H_{k-1}:H_{k-2})\cdots(H_1:H_0)} \in H.$$ □

EXERCISE 3.14. Does the previous proposition hold for non-nilpotent groups?

The following lemma is useful for performing induction on the nilpotency index of nilpotent groups.

LEMMA 3.15. *Let G be a nilpotent group of class $c \geq 2$. If $x \in G$, then the subgroup $\langle x, [G,G]\rangle$ is nilpotent of class $< c$.*

PROOF. Let $H = \langle x, [G,G]\rangle$. If $x \in [G,G]$, then there is nothing to prove. So assume that $x \notin [G,G]$. Note that

$$H = \{x^n c : n \in \mathbb{Z}, c \in [G,G]\},$$

as $[G,G]$ is normal in G. We need to show that $[H,H] \subseteq \gamma_3(G)$. Let $h = x^n c, k = x^m d \in H$ be such that $c, d \in [G,G]$. Since

$$[h, x^m] = [x^n, [c, x^m]][c, x^m] \in \gamma_4(G)\gamma_3(G) \subseteq \gamma_3(G),$$

then

$$\begin{aligned}[h,k] &= [h,x^m][x^m,[h,d]][h,d] \\ &= [x^n,[c,x^m]][c,x^m][x^m,[h,d]][h,d] \in \gamma_3(G).\end{aligned}$$ □

EXAMPLE 3.16. Let $G = \mathbb{D}_8 = \langle r, s : r^8 = s^2 = 1, srs = r^{-1}\rangle$ the dihedral group of order 16. Then G is nilpotent of class three and $[G,G] = \{1, r^2, r^4, r^6\} \simeq C_4$. The subgroup $\langle s, [G,G]\rangle \simeq \mathbb{D}_4$ is nilpotent of class two.

```
gap> G := DihedralGroup(IsPermGroup,16);;
gap> gens := GeneratorsOfGroup(G);;
gap> r := gens[1];;
gap> s := gens[2];;
gap> D := DerivedSubgroup(G);;
```

```
gap> S := Subgroup(G, Concatenation(Elements(D), [s]));;
gap> StructureDescription(S);
"D8"
gap> NilpotencyClassOfGroup(G);
3
gap> NilpotencyClassOfGroup(S);
2
```

Let us discuss a concrete application of Lemma 3.15.

THEOREM 3.17. *If G is a nilpotent group, then*

$$T(G) = \{g \in G : g^n = 1 \text{ for some } n \geq 1\}$$

is a subgroup of G.

PROOF. We proceed by induction on the nilpotency class of G. Let $a, b \in T(G)$ and

$$A = \langle a, [G,G] \rangle, \quad B = \langle b, [G,G] \rangle.$$

Since A and B are nilpotent of class $< c$ by the previous lemma, the inductive hypothesis implies that $T(A)$ is a subgroup of A and $T(B)$ is a subgroup of B. Since $T(A)$ is characteristic in A and A is normal in G, $T(A)$ is normal in G. Similarly, $T(B)$ is normal in G.

We claim that every element of $T(A)T(B)$ has finite order. If $x \in T(A)T(B)$, say $x = a_1 b_1$ with a_1 of order m, then x has finite order, as

$$x^m = (a_1 b_1)^m = (a_1 b_1 a_1^{-1})(a_1^2 b_1 a_1^{-2}) \cdots (a_1^{m-1} b_1 a_1^{-m+1}) b_1 \in T(B).$$

To see clearly what is what we did, let us work out a concrete example, say $m = 3$. In this case, we obtain the following formula:

$$\begin{aligned}(a_1 b_1)^3 &= (a_1 b_1)(a_1 b_1)(a_1 b_1) \\ &= (a_1 b_1 a_1^{-1})(a_1^2 b_1 a_1^{-2}) a_1^3 b_1 = (a_1 b_1 a_1^{-1})(a_1^2 b_1 a_1^{-2}) b_1,\end{aligned}$$

as $a_1^3 = 1$.

With this trick, we prove that ab has finite order. Hence $T(G)$ is a subgroup of G. □

Another application:

THEOREM 3.18. *Let G be a torsion-free nilpotent group and $a, b \in G$. If there exists $n \neq 0$ such that $a^n = b^n$, then $a = b$.*

PROOF. We proceed by induction on the nilpotency order c of G. The result clearly holds for abelian groups. Assume that G is nilpotent of class $c \geq 2$. Since $\langle a, [G,G] \rangle$ is a nilpotent subgroup of G of class $< c$ and $bab^{-1} = [b,a]a \in \langle a, [G,G] \rangle$, the inductive hypothesis implies that $ba = ab$, as

$$a^n = (bab^{-1})^n = b^n.$$

Thus $(ab^{-1})^n = a^n b^{-n} = 1$. Since G has no torsion, we conclude that $a = b$. □

COROLLARY 3.19. *Let G be a torsion-free nilpotent group. If $x, y \in G$ are such that $x^n y^m = y^m x^n$ for some $n, m \neq 0$, then $xy = yx$.*

PROOF. Let $a = x$ and $b = y^n x y^{-n}$. Since $a^m = b^m$, the previous theorem implies that $a = b$. Thus $xy^n = y^n x$. Apply the previous theorem again, this time with $a = y$ and $b = xyx^{-1}$. Then we conclude that $xy = yx$. □

Before proving another theorem, we recall a basic lemma about finitely generated groups.

LEMMA 3.20. *Let G be a finitely generated group and H a finite-index subgroup. Then H is finitely generated.*

PROOF. Assume that G is generated by $\{g_1,\dots,g_m\}$. Without loss of generality, we may assume that for each i there exists k such that $g_i^{-1} = g_k$.

Let $\{1 = t_1,\dots,t_n\}$ be a right transversal of H in G, so G decomposes as

$$G = \bigcup_{i=1}^{n} Ht_i \quad \text{(disjoint union)}.$$

For $i \in \{1,\dots,n\}$ and $j \in \{1,\dots,m\}$, write

$$t_i g_j = h(i,j)t_{k(i,j)}.$$

We claim that H is generated by the $h(i,j)$. Let $x \in H$. Then

$$\begin{aligned} x &= g_{i_1}\cdots g_{i_s} \\ &= (t_1 g_{i_1})g_{i_2}\cdots g_{i_s} \\ &= h(1,i_1)t_{k_1}g_{i_2}\cdots g_{i_s} \\ &= h(1,i_1)h(k_1,i_2)t_{k_2}g_{i_3}\cdots g_{i_s} \\ &= h(1,i_1)h(k_1,i_2)\cdots h(k_{s-1},i_s)t_{k_s}, \end{aligned}$$

where $k_1,\dots,k_{s-1} \in \{1,\dots,n\}$. Since $t_{k_s} \in H$ (because $x \in H$), $t_{k_s} = 1 \in H$. Hence x is generated by the $h(i,j)$. □

Now the theorem:

THEOREM 3.21. *Let G be a finitely generated torsion group that is nilpotent. Then G is finite*

PROOF. We proceed by induction on the nilpotency class c of G. The case $c = 1$ is true, as G is abelian. So assume the result holds for groups of class $c \geq 1$. Since $G/[G,G]$ is a finitely generated abelian torsion group, it is finite. Thus $[G,G]$ has finite index in G. By Lemma 3.20, $[G,G]$ is finitely generated. Moreover, $[G,G]$ is a finitely generated nilpotent torsion group of class $< c$. By the inductive hypothesis, $[G,G]$ is a finite group. Since $[G,G]$ and $G/[G,G]$ are finite, G is finite. □

Lecture 4. 07/03/2024

§ 4.1. Finite nilpotent groups. Before studying finite nilpotent groups, we need a lemma.

LEMMA 4.1. *Let G be a finite group and p a prime number dividing $|G|$. If $P \in \mathrm{Syl}_p(G)$, then*

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

PROOF. Let $H = N_G(P)$. Since P is normal in H, P is the only Sylow p-subgroup of H. To prove that $N_G(H) = H$, it is enough to see that $N_G(H) \subseteq H$. Let $g \in N_G(H)$. Since

$$gPg^{-1} \subseteq gHg^{-1} = H,$$

$gPg^{-1} \in \mathrm{Syl}_p(H)$ and H has only one Sylow p-subgroup, $P = gPg^{-1}$. Hence $g \in N_G(P) = H$. □

THEOREM 4.2. *Let G be a finite group. The following statements are equivalent:*

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

PROOF. We first prove that $(1) \implies (2)$. Let $P \in \mathrm{Syl}_p(G)$. We aim to prove that P is normal in G, that is $N_G(P) = G$. By Lemma 4.1, $N_G(N_G(P)) = N_G(P)$. Now the normalizer condition (Lemma 2.26) implies that $N_G(P) = G$.

We now prove that $(2) \implies (3)$. Let $p_1, \cdots, p_k$ be the prime factors of $|G|$. For each $i \in \{1, \ldots, k\}$, let $P_i \in \mathrm{Syl}_{p_i}(G)$. By assumption, each P_j is normal in G.

We claim that $P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$ for all j. The case $j = 1$ is trivial. So assume the result holds for some $j \geq 1$. Since

$$N = P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$$

is normal in G and it has order coprime with $|P_{j+1}|$,

$$N \cap P_{j+1} = \{1\}.$$

Hence

$$NP_{j+1} \simeq N \times P_{j+1} \simeq P_1 \times \cdots \times P_j \times P_{j+1},$$

as P_{j+1} is normal in G. Since now $P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k$ is a subgroup of G of order $|G|$, we conclude that $G = P_1 \times \cdots \times P_k$.

Finally, we prove that $(3) \implies (1)$. We just need to note that every p-group is nilpotent (Proposition 2.21) and that the direct product of nilpotent groups is nilpotent. □

EXERCISE 4.3. Let G be a finite group. Prove that if $P \in \mathrm{Syl}_p(G)$ and M is a subgroup of G such that $N_G(P) \subseteq M$, then $M = N_G(M)$.

EXERCISE 4.4. Let G be a finite group. Prove that the following statements are equivalent:

1) G is nilpotent.
2) If $H \subsetneq G$ is a subgroup of G, then $H \subsetneq N_G(H)$.
3) Every maximal subgroup of G is normal in G.

THEOREM 4.5. *Let G be a finite nilpotent group. If p is a prime number dividing $|G|$, there exist a minimal normal subgroup of order p and there exists a maximal subgroup of index p.*

PROOF. Assume that $|G| = p^\alpha m$ with $\gcd(p,m) = 1$. Write $G = P \times H$, where $P \in \mathrm{Syl}_p(G)$. Since $Z(P)$ is a non-trivial normal subgroup of P, every subgroup of $Z(P)$ that is minimal normal in G has order p (and such subgroups exist because G is finite). Since P contains a subgroup of index p, it is maximal. Hence $P \times H$ contains a maximal subgroup of index p. □

EXERCISE 4.6. Let p be a prime number and G be a non-trivial group of order p^n. Prove the following statements:

1) G has a normal subgroup of order p.
2) For every $j \in \{0,\dots,n\}$ there exists a normal subgroup of G of order p^j.

EXERCISE 4.7. Let G be a finite group. Prove that the following statements are equivalent:

1) G is nilpotent.
2) Any two elements of coprime order commute.
3) Every non-trivial quotient of G has a non-trivial center.
4) If d divides $|G|$, then there exists a normal subgroup of G of order d.

§ 4.2. The Baumslag–Wiegold theorem. The following result can be proved with elementary tools and was discovered in 2014.

THEOREM 4.8 (Baumslag–Wiegold). *Let G be a finite group such that $|xy| = |x||y|$ for all $x, y \in G$ of coprime orders. Then G is nilpotent.*

PROOF. Let $p_1,\dots,p_n$ be the prime factors of $|G|$. For each $i \in \{1,\dots,n\}$, let $P_i \in \mathrm{Syl}_{p_i}(G)$. We first prove that $G = P_1 \cdots P_n$. To prove the non-trivial inclusion, we need to show that the map

$$\psi\colon P_1 \times \cdots \times P_n \to G, \quad (x_1,\dots,x_n) \mapsto x_1 \cdots x_n$$

is surjective. We first show that ψ is injective: If $\psi(x_1,\dots,x_n) = \psi(y_1,\dots,y_n)$, then

$$x_1 \cdots x_n = y_1 \cdots y_n.$$

If $y_n \neq x_n$, then $x_1 \cdots x_{n-1} = (y_1 \cdots y_{n-1}) y_n x_n^{-1}$. Since $x_1 \cdots x_{n-1}$ has order coprime with p_n and $y_1 \cdots y_{n-1} y_n x_n^{-1}$ has order a multiple of p_n, we get a contradiction. Thus $x_n = y_n$. The same argument shows that ψ is injective. Since $|P_1 \times \cdots \times P_n| = |G|$, we conclude that ψ is bijective. In particular, ψ is surjective.

We now prove that each P_j is normal in G. Let $j \in \{1,\dots,n\}$ and $x_j \in P_j$. Let $g \in G$ and $y_j = g x_j g^{-1}$. Since $y_j \in G$, we can write $y_j = z_1 \cdots z_n$ with $z_k \in P_k$ for all k. Since the order of y_j is a power of p_j, the element $z_1 \cdots z_n$ has order a power of p_j. Thus $z_k = 1$ for all $k \neq j$. Moreover, $y_j = z_j \in P_j$. Since every Sylow subgroup of G is normal in G, we conclude that G is nilpotent. □

§ 4.3. *Itô's factorization theorem.

DEFINITION 4.9. A group G is said to be **metabelian** if $[G,G]$ is abelian.

EXERCISE 4.10. Prove that a group G is metabelian if and only if there exists a normal subgroup K of G such that K and G/K are abelian.

EXERCISE 4.11. Let G be a metabelian group. Prove the following statements:

1) If H is a subgroup of G, then H is metabelian.

2) If $f\colon G \to H$ is a group homomorphism, then $f(G)$ is metabelian.

LEMMA 4.12. *In a group, the following formulas hold:*

1) $[a,bc] = [a,b]b[a,c]b^{-1}$.

2) $[ab,c] = a[b,c]a^{-1}[a,c]$.

PROOF. This is a straightforward calculation:

$$[a,b]b[a,c]b^{-1} = aba^{-1}b^{-1}baca^{-1}c^{-1}b^{-1} = abca^{-1}c^{-1}b^{-1} = [a,bc],$$
$$a[b,c]a^{-1}[a,c] = abcb^{-1}c^{-1}a^{-1}aca^{-1}c^{-1} = abcb^{-1}a^{-1}c^{-1} = [ab,c].$$ □

EXAMPLE 4.13. The group $\mathbb{S}_3$ is metabelian, as $\mathbb{A}_3 \simeq C_3$ is a normal subgroup and the quotient $\mathbb{S}_3/\mathbb{A}_3 \simeq C_2$ an abelian group.

EXAMPLE 4.14. The group $\mathbb{A}_4$ is metabelian, as the normal subgroup

$$K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

is abelian and the quotient $\mathbb{A}_4/K \simeq C_3$ is abelian.

EXAMPLE 4.15. The group $\mathbf{SL}_2(3)$ is not metabelian, as $[\mathbf{SL}_2(3), \mathbf{SL}_2(3)] \simeq Q_8$ is not abelian:

```
gap> IsAbelian(DerivedSubgroup(SL(2,3)));
false
gap> StructureDescription(DerivedSubgroup(SL(2,3)));
"Q8"
```

THEOREM 4.16 (Itô). *Let $G = AB$ be a factorization of G with A and B abelian subgroups of G. Then G is metabelian.*

PROOF. Since $G = AB$ is a group, $AB = BA$. We claim that $[A,B]$ is a normal subgroup of G. Let $a, \alpha \in A$ and $b, \beta \in B$. Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$ be such that $\alpha b \alpha^{-1} = b_1 a_1$, $\beta a \beta^{-1} = a_2 b_2$. Since

$$\alpha[a,b]\alpha^{-1} = a(\alpha b\alpha^{-1})a^{-1}(\alpha b^{-1}\alpha^{-1}) = ab_1a_1a^{-1}a_1^{-1}b_1^{-1} = [a,b_1] \in [A,B]$$
$$\beta[a,b]\beta^{-1} = (\beta a\beta^{-1})\beta b\beta^{-1}(\beta a^{-1}\beta^{-1})b^{-1} = a_2b_2bb_2^{-1}a_2^{-1}b^{-1} = [a_2,b] \in [A,B],$$

it follows that $[A,B]$ is normal in G.

We now claim that $[A,B]$ is abelian. Since

$$\beta\alpha[a,b]\alpha^{-1}\beta^{-1} = \beta[a,b_1]\beta^{-1} = (\beta a\beta^{-1})b_1(\beta a^{-1}\beta^{-1})b_1^{-1} = [a_2,b_1],$$
$$\alpha\beta[a,b]\beta^{-1}\alpha^{-1} = \alpha[a_2,b]\alpha^{-1} = a_2(\alpha b\alpha^{-1})a_2^{-1}(\alpha b\alpha^{-1}) = [a_2,b_1],$$

a direct calculation shows that

$$[\alpha^{-1},\beta^{-1}][a,b][\alpha^{-1},\beta^{-1}]^{-1} = [a,b].$$

Two arbitrary generators of $[A,B]$ commute, so the group $[A,B]$ is abelian.

To finish the proof, note that $[G,G] = [A,B]$. In fact,

$$[a_1b_1, a_2b_2] = a_1[a_2,b_1]^{-1}a_1^{-1}a_2[a_1,b_2]a_2^{-1} \subseteq [A,B],$$

as $[A,B]$ is normal in G. □

In 1988 Sysak proved the following generalization of Itô's theorem.

THEOREM 4.17 (Sysak). *Let A and B be abelian subgroups of G. If H is a subgroup of G contained in AB, then H is metabelian.*

For the proof, see [**32**].

§ 4.4. *Nilpotent groups of class two. The following exercises go over groups of nilpotency class two.

EXERCISE 4.18. Let G be a finite group. Prove that the following statements are equivalent:

1) G is nilpotent of class ≤ 2.
2) $[G,G] \subseteq Z(G)$.
3) Any triple commutator in G is trivial.
4) The inner automorphism group of G is abelian.

EXERCISE 4.19. Let G be a nilpotent group of class two and $g \in G$. Prove that that the map $G \to G$, $x \mapsto [g,x]$, is a group homomorphism.

EXERCISE 4.20. Let G be a group. Prove that if $x,y \in G$ are such that $[x,y] \in C_G(x) \cap C_G(y)$, then

$$[x,y]^n = [x^n,y] = [x,y^n]$$

for all $n \in \mathbb{Z}$.

EXERCISE 4.21 (Hall). Let G be a class-two nilpotent group and $x,y \in G$. Prove that

$$(xy)^n = [y,x]^{n(n-1)/2} x^n y^n$$

for all $n \geq 1$.

EXERCISE 4.22. Let p be an odd prime number and P a p-group of nilpotency class ≤ 2. Prove that if $[y,x]^p = 1$ for all $x,y \in P$, then $P \to P$, $x \mapsto x^p$, is a group homomorphism.

EXERCISE 4.23. Let p be an odd prime number and P a p-group of nilpotency class ≤ 2. Prove that $\{x \in P : x^p = 1\}$ is a subgroup of P.

§ 4.5. Frattini subgroup.

DEFINITION 4.24. Let G be a group. If G has maximal subgroups, the **Frattini subgroup** is the intersection $\Phi(G)$ of all the maximal subgroups of G. Otherwise, $\Phi(G) = G$.

EXERCISE 4.25. Prove that $\Phi(G)$ is a characteristic subgroup of G.

EXAMPLE 4.26. Let $G = \mathbb{S}_3$. The maximal subgroups of G are

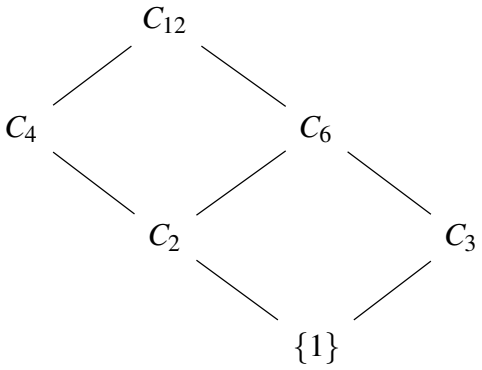
$$M_1 = \langle (123) \rangle, \quad M_2 = \langle (12) \rangle, \quad M_3 = \langle (23) \rangle, \quad M_4 = \langle (13) \rangle.$$

Hence $\Phi(G) = \{1\}$.

EXAMPLE 4.27. Let $G = \langle g \rangle \simeq C_{12}$. The subgroups of G are

$$\{1\}, \quad \langle g^6 \rangle \simeq C_2, \quad \langle g^4 \rangle \simeq C_3, \quad \langle g^3 \rangle \simeq C_4, \quad \langle g^2 \rangle \simeq C_6, \quad G.$$

Let us draw a picture:



The maximal subgroups of G are $\langle g^3 \rangle \simeq C_4$ and $\langle g^2 \rangle \simeq C_6$. Hence $\Phi(G) = \langle g^3 \rangle \cap \langle g^2 \rangle = \langle g^6 \rangle \simeq C_2$. Let us see how to do this calculation with the computer:

```
gap> G = CyclicGroup(12);;
gap> StructureDescription(FrattiniSubgroup(G));
"C2"
```

LEMMA 4.28 (Dedekind). *Let H, K and L be subgroups of G such that $H \subseteq L \subseteq G$. Then $HK \cap L = H(K \cap L)$.*

PROOF. One inclusion is trivial. Let us prove then that $HK \cap L \subseteq H(K \cap L)$. If $x = hk \in HK \cap L$ with $x \in L$, $h \in H$ and $k \in K$, then $k = h^{-1}x \in L \cap K$, as $H \subseteq L$. Thus $x = hk \in H(L \cap K)$. □

LEMMA 4.29. *Let G be a finite group and H be a subgroup of G such that $G = H\Phi(G)$. Then $H = G$.*

PROOF. If $H \neq G$, let M be a maximal subgroup of G such that $H \subseteq M$. Since $\Phi(G) \subseteq M$, $G = H\Phi(G) \subseteq M$, a contradiction. □

PROPOSITION 4.30. *Let N be a normal subgroup of a finite group G. Then $\Phi(N) \subseteq \Phi(G)$.*

PROOF. Since $\Phi(N)$ is characteristic in N and N is normal in G, $\Phi(N)$ is normal in G. If there exists a maximal subgroup M such that $\Phi(N) \not\subseteq M$, then $\Phi(N)M = G$. (This happens because, otherwise, $M = \Phi(N)M \supseteq \Phi(N)$.) By Dedekind's lemma (with $H = \Phi(N)$, $K = M$ and $L = N$),

$$N = G \cap N = (\Phi(N)M) \cap N = \Phi(N)(M \cap N).$$

By Lemma 4.29 (with $G = N$ and $H = M \cap N$), $\Phi(N) \subseteq N \subseteq M$, a contradiction. Hence every maximal subgroup of G contains $\Phi(N)$ and therefore $\Phi(G) \supseteq \Phi(N)$. □

The following proposition states that the elements of the Frattini subgroup are the **non-generators** of the group.

PROPOSITION 4.31. *Let G be a finite group. Then*

$$\Phi(G) = \{x \in G : \text{if } G = \langle x, Y \rangle \text{ for some } Y \subseteq G, \text{ then } G = \langle Y \rangle\}.$$

Proof. We first prove $\supseteq$. Let $x \in \{x \in G : \text{if } G = \langle x, Y\rangle \text{ for some } Y \subseteq G, \text{ then } G = \langle Y\rangle\}$. If M is a maximal subgroup of G such that $x \notin M$, then, since $G = \langle x, M\rangle$, we obtain that $G = \langle M\rangle = M$, a contradiction. Thus $x \in M$ for all maximal subgroup M of G. Hence $x \in \Phi(G)$.

We now prove $\subseteq$. Let $x \in \Phi(G)$ be such that $G = \langle x, Y\rangle$ for some subset Y of G. If $G \neq \langle Y\rangle$, there exists a maximal subgroup M such that $\langle Y\rangle \subseteq M$. Since $x \in M$, $G = \langle x, Y\rangle \subseteq M$, a contradiction. □

Example 4.32. For a prime number p, let G be an elementary p-group, that is $G \simeq C_p^m$ for some $m \geq 1$. Assume that $G = \langle x_1\rangle \times \cdots \times \langle x_m\rangle$ with $\langle x_j\rangle \simeq C_p$. We claim that $\Phi(G)$ is trivial. For $j \in \{1, \ldots, m\}$, let $n_j \in \{1, \ldots, p-1\}$. Since

$$\{x_1, \ldots, x_{j-1}, x_j^{n_j}, x_{j+1}, \ldots, x_m\}$$

generates G and $\{x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_m\}$ does not, $x_j^{n_j} \notin \Phi(G)$ by Proposition 4.31. Hence $\Phi(G) = \{1\}$.

Theorem 4.33 (Frattini). *Let G be a finite group. Then $\Phi(G)$ is nilpotent.*

Proof. Let $P \in \mathrm{Syl}_p(\Phi(G))$ for some prime number p. Since $\Phi(G)$ is normal in G, Lemma 1.28 (Frattini's argument) implies that $G = \Phi(G)N_G(P)$. By Lemma 4.29, $G = N_G(P)$. Since every Sylow subgroup of $\Phi(G)$ is normal in G, $\Phi(G)$ is nilpotent. □

Exercise 4.34. Let G be a group and M be a normal subgroup of G. Prove that if M is maximal, then G/M is cyclic of prime order.

Theorem 4.35 (Gaschütz). *If G is a finite group, then*

$$[G, G] \cap Z(G) \subseteq \Phi(G).$$

Proof. Let $D = [G, G] \cap Z(G)$. Assume that D is not contained in $\Phi(G)$. Since $\Phi(G)$ is contained in every maximal subgroup of G, there is a maximal subgroup M of G not containing D. Then $G = MD$. Since $D \subseteq Z(G)$, M is normal in G, as $g = md \in G = MD$ implies

$$gMg^{-1} = (md)Md^{-1}m^{-1} = mMm^{-1} = M.$$

Since G/M is cyclic of prime order, G/M is, in particular, abelian and hence $[G, G] \subseteq M$. Therefore $D \subseteq [G, G] \subseteq M$, a contradiction. □

Lemma 4.36. *Let G be a finite group and $P \in \mathrm{Syl}_p(G)$. If H is a subgroup of G such that $N_G(P) \subseteq H$, then $N_G(H) = H$.*

Proof. Let $x \in N_G(H)$. Since $P \in \mathrm{Syl}_p(H)$ and $Q = xPx^{-1} \in \mathrm{Syl}_p(H)$, the second Sylow's theorem implies that there exists $h \in H$ such that $hQh^{-1} = (hx)P(hx)^{-1} = P$. Then $hx \in N_G(P) \subseteq H$ and hence $x \in H$. □

Theorem 4.37 (Wielandt). *A finite group G is nilpotent if and only if $[G, G] \subseteq \Phi(G)$.*

Proof. Assume that $[G, G] \subseteq \Phi(G)$. Let $P \in \mathrm{Syl}_p(G)$. If $N_G(P) \neq G$, then $N_G(P) \subseteq M$ for some maximal subgroup M of G. If $g \in G$ and $m \in M$, then, since

$$gmg^{-1}m^{-1} = [g, m] \in [G, G] \subseteq \Phi(G) \subseteq M,$$

M is normal in G. Furthermore $N_G(P) \subseteq M$. By Lemma 4.36,

$$G = N_G(M) = M,$$

a contradiction. Thus $N_G(P) = G$ and every Sylow subgroup of G si normal in G. Therefore G is nilpotent.

Conversely, assume that G is nilpotent. Let M be a maximal subgroup of G. Since M is normal in G and maximal, G/M has no proper non-trivial subgroups. Then $G/M \simeq C_p$ for some prime number p. In particular, G/M is abelian and $[G,G] \subseteq M$. Since $[G,G]$ is contained in every maximal subgroup of G, $[G,G] \subseteq \Phi(G)$. □

THEOREM 4.38. *A finite group G is nilpotent if and only if $G/\Phi(G)$ is nilpotent.*

PROOF. If G is nilpotent, then $G/\Phi(G)$ is nilpotent. Conversely, assume that $G/\Phi(G)$ is nilpotent. Let $P \in \mathrm{Syl}_p(G)$. Since $\Phi(G)P/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$ and $G/\Phi(G)$ is nilpotent, $\Phi(G)P/\Phi(G)$ is a normal subgroup of $G/\Phi(G)$. By the correspondence theorem, $\Phi(G)P$ is a normal subgroup of G. Since $P \in \mathrm{Syl}_p(\Phi(G)P)$, Frattini's argument (Lemma 1.28) implies that

$$G = \Phi(G)PN_G(P) = \Phi(G)N_G(P),$$

as $P \subseteq N_G(P)$. Thus $G = N_G(P)$ by Lemma 4.29). Hence P is normal in G and therefore G is nilpotent. □

Lecture 5. 14/03/2024

THEOREM 5.1 (Hall). *Let G be a finite group with a normal subgroup N. If both N and $G/[N,N]$ are nilpotent, then G is nilpotent.*

PROOF. Since N is nilpotent, $[N,N] \subseteq \Phi(N)$ by Wielandt's theorem 4.37. By Proposition 4.30, $[N,N] \subseteq \Phi(N) \subseteq \Phi(G)$. By the universal property, there exists a surjective group homomorphism $G/[N,N] \to G/\Phi(G)$ such that the diagram

$$\begin{array}{ccc} G & \longrightarrow & G/\Phi(G) \\ \downarrow & \nearrow & \\ G/[N,N] & & \end{array}$$

is commutative. Since $G/[N,N]$ is nilpotent, $G/\Phi(G)$ is nilpotent. Thus G is nilpotent by the previous theorem. □

DEFINITION 5.2. A **minimal generating set** of a group G is a set X of generators of G such that no proper subset of X generates G.

Note that a minimal generating set does not necessarily have minimal size.

EXAMPLE 5.3. Let $G = \langle g \rangle \simeq C_6$. If $a = g^2$ and $b = g^3$, then $\{a,b\}$ is a minimal generating set of G that does not have minimal size, as $G = \langle ab \rangle$.

For a prime number p, we write $\mathbb{F}_p$ to denote the field of p elements.

LEMMA 5.4. *Let p be a prime number and G be a finite p-group. Then $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$.*

PROOF. Let K be a maximal subgroup of G. Since G is nilpotent (see Proposition 2.21), K is normal in G (Exercise 4.4). Thus $G/K \simeq C_p$ because it is a simple p-group.

It is enough to prove that $G/\Phi(G)$ is an elementary abelian p-group. It is a p-group because G is a p-group. Let $K_1, \ldots, K_m$ be the maximal subgroups of G. If $x \in G$, then $x^p \in K_j$ for all $j \in \{1, \ldots, m\}$. Hence $x^p \in \Phi(G) = \cap_{j=1}^m K_j$. Moreover, $G/\Phi(G)$ is abelian, as $[G,G] \subseteq \Phi(G)$ because G is nilpotent (Wielandt's theorem 4.37). □

THEOREM 5.5 (Burnside). *Let p be a prime number and G a finite p-group. If X is a minimal generating set of G, then $|X| = \dim G/\Phi(G)$.*

PROOF. By Lemma 5.4, $G/\Phi(G)$ is a vector space over $\mathbb{F}_p$. Let $\pi\colon G \to G/\Phi(G)$ be the canonical map and $\{x_1, \ldots, x_n\}$ be a minimal generating set of G. We claim that $\{\pi(x_1), \ldots, \pi(x_n)\}$ is a linearly independent subset of $G/\Phi(G)$. Assume this is not the case. Without loss of generality, let us assume that $\pi(x_1) \in \langle \pi(x_2), \ldots, \pi(x_n) \rangle$. There exists $y \in \langle x_2, \ldots, x_n \rangle$ such that $x_1 y^{-1} \in \Phi(G)$. Since G is generated by $\{x_1 y^{-1}, x_2, \ldots, x_n\}$ and $x_1 y^{-1} \in \Phi(G)$, Proposition 4.31 implies that G is generated by $\{x_2, \ldots, x_n\}$, a contradiction to the minimality of $\{x_1, \ldots, x_n\}$. Therefore $n = \dim G/\Phi(G)$. □

EXERCISE 5.6. Let p be a prime number and G a finite p-group. Prove that if $x \notin \Phi(G)$, then x belongs to some minimal set of generators of G.

§ 5.1. The Fitting subgroup.

DEFINITION 5.7. Let G be a finite group and p be a prime number. The **p-radical** of G is the subgroup

$$O_p(G) = \bigcap_{P \in \mathrm{Syl}_p(G)} P.$$

LEMMA 5.8. *Let G be a finite group and p be a prime number. The following statements hold:*

1) *$O_p(G)$ is normal in G.*

2) *If N is a normal subgroup of G contained in some $P \in \mathrm{Syl}_p(G)$, then $N \subseteq O_p(G)$.*

PROOF. Let $P \in \mathrm{Syl}_p(G)$. Let G act on G/P by left multiplication. There is a group homomorphism $\rho\colon G \to \mathbb{S}_{G/P}$ with kernel

$$\begin{aligned}
\ker\rho &= \{x \in G : \rho_x = \mathrm{id}\} \\
&= \{x \in G : xgP = gP \ \forall g \in G\} \\
&= \{x \in G : x \in gPg^{-1} \ \forall g \in G\} \\
&= \bigcap_{g \in G} gPg^{-1} \\
&= O_p(G).
\end{aligned}$$

Then $O_p(G)$ is normal in G.

Let N be a normal subgroup of G such that $N \subseteq P$. Since $N = gNg^{-1} \subseteq gPg^{-1}$ for all $g \in G$, we conclude that $N \subseteq O_p(G)$. □

DEFINITION 5.9. Let G be a finite group and $p_1, \ldots, p_k$ be the prime divisors of $|G|$. The **Fitting subgroup** of G is the subgroup

$$F(G) = O_{p_1}(G) \cdots O_{p_k}(G)$$

EXERCISE 5.10. Prove that $F(G)$ is characteristic in G.

EXAMPLE 5.11. Let $G = \mathbb{S}_3$. Then $O_2(G) = \{1\}$ and $O_3(G) = \langle(123)\rangle$. Hence $F(G) = \langle(123)\rangle$.

THEOREM 5.12 (Fitting). *Let G be a finite group. Then $F(G)$ is a nilpotent and normal in G. Moreover, $F(G)$ contains every nilpotent normal subgroup of G.*

PROOF. By definition, $|F(G)| = \prod_p |O_p(G)|$. Since $O_p(G) \in \mathrm{Syl}_p(F(G))$, we conclude that $F(G)$ is nilpotent, as it contains a normal Sylow p-subgroup for every prime p. Hence $F(G)$ is nilpotent by Theorem 4.2.

Let N be a nilpotent normal subgroup of G and $P \in \mathrm{Syl}_p(N)$. Since N is nilpotent, P is normal in N and hence P is the only Sylow p-subgroup of N. Thus P is characteristic in N and P is normal in G. Since N is nilpotent, N is a direct product of its Sylow subgroups. Therefore $N \subseteq O_p(G)$ by Lemma 5.8. □

COROLLARY 5.13. *If G is a finite group, then $Z(G) \subseteq F(G)$.*

PROOF. Since $Z(G)$ is nilpotent (in fact, it is abelian) and normal in G, by Fitting's theorem 5.12 we conclude that $Z(G) \subseteq F(G)$ □

COROLLARY 5.14 (Fitting). *Let K and L be nilpotent normal subgroups of a finite group G. Then KL is nilpotent.*

PROOF. By Fitting's theorem 5.12, $K \subseteq F(G)$ and $L \subseteq F(G)$. Then $KL \subseteq F(G)$ and KL is nilpotent, as $F(G)$ is nilpotent. □

COROLLARY 5.15. *Let N be a normal subgroup of a finite group G. Then $N \cap F(G) = F(N)$.*

PROOF. Since $F(N)$ is characteristic in N, $F(N)$ is normal in G. Then $F(N) \subseteq N \cap F(G)$ because $F(N)$ is nilpotent. Conversely, since $F(G)$ is normal in G, the subgroup $F(G) \cap N$ is normal in N. Since $F(G) \cap N$ is nilpotent, $F(G) \cap N \subseteq F(N)$. □

We now discuss an application to finite solvable groups.

THEOREM 5.16. *Let G be a non-trivial solvable group. Every normal non-trivial subgroup N contains a normal abelian non-trivial subgroup. Moreover, this subgroup is contained in $F(N)$.*

PROOF. Note that $N \cap G^{(0)} = N \neq \{1\}$. Since G is solvable, there exists $m \geq 1$ such that $N \cap G^{(m)} = \{1\}$. Let n be the largest positive integer such that $N \cap G^{(n)} \neq \{1\}$. Since $[N,N] \subseteq N$ and $[G^{(n)}, G^{(n)}] = G^{(n+1)}$,

$$[N \cap G^{(n)}, N \cap G^{(n)}] \subseteq N \cap G^{(n+1)} = \{1\}.$$

Then $N \cap G^{(n)}$ is an abelian subgroup of G. Moreover, it is normal and nilpotent. Hence

$$N \cap G^{(n)} \subseteq N \cap F(G) = F(N). \qquad \square$$

THEOREM 5.17. *If N is a minimal normal subgroup of a finite group G, then $F(G) \subseteq C_G(N)$.*

PROOF. By Fitting's theorem 5.12, $F(G)$ is a normal nilpotent group. The subgroup $N \cap F(G)$ is normal in G. Moreover, $[F(G),N] \subseteq N \cap F(G)$. If $N \cap F(G) = \{1\}$, then $[F(G),N] = \{1\}$. Otherwise, $N = N \cap F(G) \subseteq F(G)$ by the minimality of N. By Hirsch's theorem, $N \cap Z(F(G)) \neq \{1\}$ Since $Z(F(G))$ is characteristic in $F(G)$ and $F(G)$ is normal in G, $Z(F(G))$ is normal in G. Since $\{1\} \neq N \cap Z(F(G))$ is normal in G, the minimality of N implies that $N = N \cap Z(F(G)) \subseteq Z(F(G))$. Hence $[F(G),N] = \{1\}$. □

COROLLARY 5.18. *Let G be a finite solvable group. The following statements hold:*

1) *If N is a minimal normal subgroup, then $N \subseteq Z(F(G))$.*
2) *If H is a non-trivial normal subgroup, then $H \cap F(G) \neq \{1\}$.*

PROOF. Let us prove the first claim. Since N is a p-group by Lemma 1.22, N is nilpotent and hence $N \subseteq F(G)$. Moreover, $F(G) \subseteq C_G(N)$ by the previous theorem. Therefore $N \subseteq Z(F(G))$.

Let us prove now the second claim. The subgroup H contains a minimal normal subgroup N and $N \subseteq F(G)$. Then $H \cap F(G) \neq \{1\}$. □

THEOREM 5.19. *Let G be a finite group. The following statements hold:*

1) *$\Phi(G) \subseteq F(G)$ and $Z(G) \subseteq F(G)$.*
2) *$F(G)/\Phi(G) \simeq F(G/\Phi(G))$.*

PROOF. Let us prove the first claim. Since $\Phi(G)$ is normal in G, nilpotent by Frattini's Theorem 4.33 and $F(G)$ contains every normal nilpotent subgroup of G, $\Phi(G) \subseteq F(G)$. Moreover, $Z(G)$ is normal in G and nilpotent. Hence $Z(G) \subseteq F(G)$.

Let us prove the second claim. Let $\pi\colon G \to G/\Phi(G)$ be the canonical map. Since $F(G)$ is nilpotent, $\pi(F(G))$ is nilpotent. Hence

$$\pi(F(G)) \subseteq F(G/\Phi(G))$$

by Fitting's Theorem 5.12. Let $H = \pi^{-1}(F(G/\Phi(G)))$. By the correspondence theorem, H is a normal subgroup of G containing $\Phi(G)$. If $P \in \mathrm{Syl}_p(H)$, then $\pi(P) \in \mathrm{Syl}_p(\pi(H))$. In fact, $\pi(P) \simeq P/P\cap\Phi(G)$ is a p-group and $(\pi(H) : \pi(P))$ is coprime with p because

$$(\pi(H) : \pi(P)) = \frac{|\pi(H)|}{|\pi(P)|} = \frac{|H/\Phi(G)|}{|P/P\cap\Phi(G)|} = \frac{(H : P)}{(\Phi(G) : P\cap\Phi(G))}$$

divides $(H : P)$, a number coprime with p. Since $\pi(H)$ is nilpotent, $\pi(P)$ is characteristic in $\pi(H)$. Then $\pi(P)$ is normal in $\pi(G) = G/\Phi(G)$ and $P\Phi(G) = \pi^{-1}(\pi(P))$ is normal in G. Since $P \in \mathrm{Syl}_p(P\Phi(G))$, Frattini's argument (Lemma 1.28) implies that $G = \Phi(G)N_G(P)$. Therefore P is normal in G by Lemma 4.29. Moreover, P is normal in H. Since P is nilpotent and normal in G, $P \subseteq F(G)$ by Fitting's theorem 5.12. Hence $H \subseteq F(G)$ and $F(G/\Phi(G)) = \pi(H) \subseteq \pi(F(G))$. □

§ 5.2. *Mann subgroup. Let G be a finite group with conjugacy classes sizes

$$1 = n_1 < n_2 < \cdots < n_k.$$

For example, for $G = \mathbb{S}_3$ one has $k = 3$ and $(n_1, n_2, n_3) = (1, 2, 3)$. How the number k of class sizes affect the structure of the group?

Open problem 5.20. What is the connection between the conjugacy classes sizes and the nilpotency of a group?

For example, if $k = 1$, then G is abelian. Itô proved that if $k = 2$, then G is nilpotent; see [**23**]. And Ishikawa proved that the nilpotency class of G is at most three.

Definition 5.21. Let G be a finite group. The **Mann subgroup** $M(G)$ is defined as the subgroup of G generated by all elements lying in conjugacy classes of size $\leq n_2$.

Ishikawa's theorem follows from the following theorem.

Theorem 5.22 (Mann). *Let G be a nilpotent finite group. Then $M(G)$ has nilpotency class ≤ 3.*

Proof. See [**22**, Theorem 4.14]. □

Lecture 6. 21/03/2024

§ 6.1. Super-solvable groups.

DEFINITION 6.1. A group G is said to be **super-solvable** if there exists a sequence

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

of normal subgroups of G such that every quotient G_{i-1}/G_i is cyclic.

In the previous definition, we do not require the group to be finite. Hence the quotients could be finite cyclic groups or isomorphic to $\mathbb{Z}$.

EXAMPLE 6.2. The dihedral group $\mathbb{D}_n$ of order $2n$ is super-solvable, as

$$\mathbb{D}_n \supseteq \langle r \rangle \supseteq \{1\}$$

is a sequence of normal subgroups with cyclic factors.

Every super-solvable group is solvable. See Exercise 1.6.

EXAMPLE 6.3. The alternating group $\mathbb{A}_4$ solvable but not super-solvable. The only proper non-trivial normal subgroup of $\mathbb{A}_4$ is

$$\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2.$$

Thus $\mathbb{A}_4$ does not have a sequence of normal subgroups with cyclic factors.

EXAMPLE 6.4. The group $\mathbf{SL}_2(3)$ is solvable but not super-solvable. Here is a computer verification:

```
gap> IsSolvable(SL(2,3));
true
gap> IsSupersolvable(SL(2,3));
false
```

EXERCISE 6.5. Prove the following statements:

1) Every subgroup of a super-solvable group is super-solvable.
2) Quotients of super-solvable groups are super-solvable.

EXERCISE 6.6. Prove that the direct product of super-solvable groups is super-solvable.

EXERCISE 6.7. Let H and K be normal subgroups of a group G such that G/K and G/H are super-solvable. Prove that $G/H \cap K$ is super-solvable.

EXERCISE 6.8. Let N be a cyclic normal subgroup of G. If G/N is super-solvable, then G is super-solvable.

THEOREM 6.9. *Let G be a super-solvable non-trivial group. Then G admits a sequence*

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

of normal subgroups such that every quotient G_{i-1}/G_i is cyclic of prime order or isomorphic to $\mathbb{Z}$.

PROOF. Let $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ be a sequence of normal subgroups of G such that every quotient G_{i-1}/G_i is cyclic. Let $i \in \{1,\ldots,n\}$ be such that $G_{i-1}/G_i \simeq C_n$ for some non-prime n and let $\pi\colon G_{i-1} \to G_{i-1}/G_i$ be the canonical map. Let p be a prime divisor of n and H be a subgroup of G such that $\pi(H)$ is a subgroup of G_{i-1}/G_i of order p. By the correspondence theorem, $G_i \subseteq H \subseteq G_{i-1}$.

We claim that H is normal in G. Let $g \in G$. Since $\pi(gHg^{-1})$ is a subgroup of order p of the cyclic group G_{i-1}/G_i, $\pi(gHg^{-1}) = \pi(H)$. Then $gHg^{-1} = G_iH \subseteq H$ and hence $gHg^{-1} = H$.

Note that H/G_i is cyclic of prime order, as

$$H/G_i = H/H \cap G_i \simeq \pi(H) \simeq C_p.$$

Moreover, G_{i-1}/H is cyclic, as

$$G_{i-1}/H \simeq \frac{G_{i-1}/G_i}{H/G_i}$$

is the quotient of a cyclic group.

We have shown that by adding H to our sequence of normal subgroups, we obtain a sequence with cyclic factors where H/G_i is cylic of prime order. Repeating this procedure, we obtain the desired result. □

Let us discuss an immediate application.

COROLLARY 6.10. *A finite super-solvable group admits a sequence of normal subgroups where each quotient is cyclic of prime order.*

We now discuss other properties of super-solvable groups.

THEOREM 6.11. *Let G be a super-solvable group. The following statement hold:*

1) *If N is minimal normal in G, then $N \simeq C_p$ for some prime number p.*

2) *If M is maximal in G, then $(G : M) = p$ for some prime number p.*

PROOF. Let us prove the first claim. Since G is super-solvable, there exists a sequence

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{1\}$$

of normal subgroups with cyclic factors. Since each $G_i \cap N$ is a normal subgroup of G contained in N, the minimality implies that each $G_i \cap N$ is either trivial or equal to N. Moreover, $N \cap G_0 = N$ and $N \cap G_n = \{1\}$. Let j be the smallest positive integer such that $N \cap G_j = \{1\}$. Since $N \subseteq G_{j-1}$ (because $N \cap G_{j-1} = N$), the composition

$$N \hookrightarrow G_{j-1} \to G_{j-1}/G_j$$

is an injective group homomorphism, as its kernel is equal $N \cap G_j = \{1\}$. Thus N is cyclic, as it is isomorphic to a subgroup of the cyclic group G_{i-1}/G_i. If $G_{i-1}/G_i \simeq \mathbb{Z}$, then $N \simeq \mathbb{Z}$, a contradiction to the fact that N is minimal normal. (For example, $2\mathbb{Z}$ is characteristic subgroup of $\mathbb{Z}$ and hence it is normal in G. Thus N is cyclic and finite. Hence $N \simeq C_p$.)

We now prove the second claim. Let M be a maximal subgroup of G. If M is normal in G, then G/M does not contain non-trivial proper subgroups. Then $G/M \simeq C_p$ for some prime number p. Assume that M is not normal in G. Let $H = \cap_{g\in G} gMg^{-1}$ and $\pi\colon G \to G/H$ be the canonical map. Since $\pi(M)$ is maximal in $\pi(G) = G/H$ and

$$(G : M) = (G/H : M/H) = (G/H : M/H \cap M) = (\pi(G) : \pi(M)),$$

we may assume that M does not contain non-trivial normal subgroups of G (if needed, we just replace G by G/H). Since G is super-solvable, there exists a sequence $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ of

normal subgroups of G with factors either cyclic of prime order or isomorphic to $\mathbb{Z}$. Let $N = G_{n-1}$. Since N is cyclic, every subgroup of N is characteristic in N and hence normal in G. In particular, $M \cap N$ is normal in G and therefore $M \cap N = \{1\}$. Since $M \subseteq NM \subseteq G$, the maximality of M implies that either $M = NM$ or $G = NM$. Since $N \subseteq NM = M$ yields a contradiction, we conclude that $G = NM$.

If $N \simeq C_p$ for some prime p, then $(G : M) = p$ and the proof is complete. Assume that $N \simeq \mathbb{Z}$. Let H be a proper non-trivial subgroup of N. Since H is characteristic in N, H is normal in G. Since $M \subseteq HM \subseteq NM = G$, the maximality of M implies that either $HM = M$ or $HM = G$. Since $HM = M$ implies $H \subseteq M \cap N = \{1\}$, we may assume that $HM = G$. If $n \in N \setminus H$, then $n = hm$ for some $h \in H$ and $m \in M$. Then $h = n$, as $h^{-1}n \in N \cap M = \{1\}$, a contradiction.

□

EXERCISE 6.12. Let G be a super-solvable group. Prove the following statements:

1) The commutator subgroup $[G, G]$ is nilpotent.

2) If G is non-abelian, there exists a normal subgroup $N \neq G$ such that $Z(G) \subsetneq N$.

There are solvable groups with a non-nilpotent derived subgroup.

EXAMPLE 6.13. The group $\mathbb{S}_4$ is solvable and $[\mathbb{S}_4, \mathbb{S}_4] = \mathbb{A}_4$ is not nilpotent.

PROPOSITION 6.14. *Let p be a prime number. Every finite p-group is super-solvable.*

PROOF. Let G be a minimal counterexample. We may assume that $|G| = p^n$ for some $n > 1$ (otherwise, if $n = 1$, then G is trivially super-solvable). The group G is nilpotent and contains a normal subgroup N of order p. Moreover, since $|G/N| = p^{n-1}$, the group G/N is super-solvable. Since N is cyclic and G/N is super-solvable, G is super-solvable by Exercise 6.8. □

EXERCISE 6.15. Prove that finite nilpotent groups are super-solvable.

THEOREM 6.16. *Super-solvable groups have maximal subgroups.*

PROOF. We proceed by induction on the length of the super-solvable series. The claim holds for groups with a super-solvable series of length one, as in this case we are dealing with cyclic groups. So let G be a group admitting a sequence

$$G = G_0 \supseteq \cdots \supseteq G_k = \{1\}$$

and suppose the theorem holds for super-solvable groups with super-solvable series of length $< k$. Note that G_{k-1} is normal in G. Let $\pi \colon G \to G/G_{k-1}$ be the canonical map. The sequence

$$G/G_{k-1} = \pi(G) \supseteq \pi(G_1) \supseteq \cdots \supseteq \pi(G_{k-1}) = \{1\}$$

has length $< k$ and proves the super-solvability of $\pi(G)$. By the inductive hypothesis, G/G_{k-1} admits maximal subgroups. By the correspondence theorem, G admits maximal subgroups. □

Solvable or nilpotent groups do not always admit maximal subgroups. Can you give an example?

DEFINITION 6.17. A group G satisfies the **maximal condition on subgroups** if for every non-empty subset $\mathscr{S}$ of subgroups contains a maximal element (i.e. a subgroup not contained in any other subgroup of $\mathscr{S}$).

EXERCISE 6.18. A group satisfies the maximal condition on subgroups if and only if every subgroup of G is finitely generated.

EXERCISE 6.19. Let H be a subgroup of a group G. If G satisfies the maximal condition on subgroups, then so does H.

EXERCISE 6.20. Let G be a group and N be a normal subgroup of G. If G/N and N satisfy the maximal condition on subgroups, then so does G.

PROPOSITION 6.21. *Super-solvable groups satisfy the maximal condition on subgroups. In particular, every super-solvable group is finitely generated.*

PROOF. We proceed by induction on the length of the super-solvable sequence. If the length is one, the result holds as the group is cyclic. So assume the result holds for super-solvable groups with super-solvable series of length $\leq n-1$. Let G be a non-trivial super-solvable group and

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = \{1\}$$

a sequence of normal subgroups of G with cyclic factors. Since G_1 is super-solvable (Exercise 6.5), G_1 satisfies the maximal condition on subgroups by the inductive hypothesis. By Exercise 6.20, G satisfies the maximal condition on subgroups, as G/G_1 is cyclic. □

EXAMPLE 6.22. The abelian group $\mathbb{Q}$ is nilpotent but not super-solvable, as it is not finitely generated.

If G is a group and $x_1, \ldots, x_{n+1} \in G$, let

$$[x_1, x_2 \ldots, x_{n+1}] = [x_1, [x_2, \ldots, x_{n+1}]], \quad n \geq 1.$$

We will prove in Theorem 6.25 that nilpotent groups are super-solvable if and only if they are finitely generated. For this, we need two lemmas.

LEMMA 6.23. *Let G be a finite generated group, say $G = \langle X \rangle$ for some finite set X. For $n \geq 2$, let*

$$G_n = \langle g[x_1, \ldots, x_n]g^{-1} : x_1, \ldots, x_n \in X, g \in G \rangle.$$

Then $G_n = \gamma_n(G)$ for all $n \geq 2$.

PROOF. Note that each G_n is normal in G. We proceed by induction on n. The case $n = 2$ is trivial. So let us assume that $\gamma_{n-1}(G) = G_{n-1}$ for some $n \geq 2$. Let $x_1, \ldots, x_n \in X$. Since $[x_1, \ldots, x_n] \in \gamma_n(G)$, $G_{n-1} \subseteq \gamma_n(G)$. Let $N = G_n$ and $\pi \colon G \to G/N$ be the canonical map. The group G/N is finitely generated. Since

$$[\pi(x_1), [\pi(x_2), \ldots, \pi(x_n)]] = \pi([x_1, \ldots, x_n]) = 1,$$

we obtain that $\pi([x_2, \ldots, x_n]) \in Z(G/N)$. Hence $\pi(g[x_2, \ldots, x_n]g^{-1}) = 1$ for all $g \in G$. By the inductive hypothesis,

$$\pi(\gamma_{n-1}(G)) = \pi(G_{n-1}) \subseteq Z(G/N).$$

Since

$$\pi(\gamma_n(G)) = \pi([G, \gamma_{n-1}(G)]) = [\pi(G), \pi(\gamma_{n-1}(G))] = \{1\},$$

we conclude that $\gamma_n(G) \subseteq N = G_n$. □

LEMMA 6.24. *Let G be a finitely generated group. Then $\gamma_n(G)/\gamma_{n+1}(G)$ is finitely generated.*

PROOF. Assume that $G = \langle X \rangle$ for some finite set X. Write

$$g[x_1,\dots,x_n]g^{-1} = [g,[x_1,\dots,x_n]][x_1,\dots,x_n].$$

By Lemma 6.23, $[g,[x_1,\dots,x_n]] \in \gamma_{n+1}(G) = G_{n+1}$. Then

$$g[x_1,\dots,x_n]g^{-1} \equiv [x_1,\dots,x_n] \bmod \gamma_{n+1}(G).$$

Hence $\gamma_n(G)/\gamma_{n+1}(G)$ is generated by the finite set

$$\{[x_1,\dots,x_n]\gamma_{n+1}(G) : x_1,\dots,x_n \in X\}. \qquad \square$$

THEOREM 6.25. *Let G be a nilpotent group. Then G is super-solvable if and only if G is finitely generated.*

PROOF. If G is super-solvable, it is then finitely generated by Proposition 6.21.

Now assume that the nilpotent group G is finitely generated. By Lemma 6.24, each quotient $\gamma_n(G)/\gamma_{n+1}(G)$ is finitely generated, say by the elements $y_1,\dots,y_m$. Let $\pi\colon G \to G/\gamma_{n+1}(G)$ the canonical map. For $j \in \{1,\dots,m\}$, let

$$K_j = \langle \gamma_{n+1}(G), y_1,\dots,y_j \rangle.$$

Since $[G,K_j] \subseteq [G,\gamma_n(G)] = \gamma_{n+1}(G)$, we obtain that $\pi(K_j)$ is central in $\pi(G)$. Thus $\pi(K_j)$ is normal in $\pi(G)$. Hence K_j is normal in G. Each quotient K_j/K_{j-1} is cyclic and generated by y_jK_{j-1}. Therefore, in between $\gamma_n(G)$ and $\gamma_{n+1}(G)$, we have constructed a sequence of normal subgroups of G with cyclic factors. Since G is nilpotent, there exists an integer c such that $\gamma_{c+1}(G) = \{1\}$. Hence G is super-solvable. $\square$

COROLLARY 6.26. *Every finitely generated nilpotent group satisfies the maximal condition on subgroups.*

PROOF. This is an immediate consequence of Proposition 6.21 and Theorem 6.25. $\square$

THEOREM 6.27. *Let G be a nilpotent finitely generated group. Then $T(G)$ is finite.*

PROOF. Since G is nilpotent, G satisfies the maximal condition on subgroups (Corollary 6.26). Thus every subgroup of G is finitely generated. Since $T(G)$ is a subgroup (Theorem 3.17), it is a torsion finitely generated group. Hence $T(G)$ is finite by Theorem 3.21. $\square$

§ 6.2. *Huppert's super-solvable theorem.

THEOREM 6.28 (Huppert). *Let G be a finite group such that all its maximal subgroups are of prime index. Then G is super-solvable.*

PROOF. See [**16**, Theorem 10.5.8]. $\square$

§ 6.3. *Formanek's zero divisors theorem. We start recalling a conjecture formulated by Kaplansky as [**24**, Problem 6] in 1957.

CONJECTURE 6.29 (Kaplansky). Let K be a field and G be a torsion-free group. Then $K[G]$ has no zero divisors.

In 1973 Formanek proved the following result:

THEOREM 6.30 (Formanek). *Let G be a torsion-free super-solvable group and K be a field. Then $K[G]$ has no zero divisors.*

PROOF. See [**27**, Theorem 13.3.9]. □

Conjecture 6.29 is also known to hold, for example, when G admits a bi-order (proved by Malcev and independently by Neumann), when G is polycyclic-by-finite (proved by Brown and Farkas–Snider), or when G has the unique product property (proved by Cohen). In full generality, the conjecture is still open. See [**27**, Chapter 13] for more information.

Lecture 7. 28/03/2024

§ 7.1. The Schur–Zassenhaus theorem. Recall that a group Q **acts by automorphisms** on a group K if there exists a map $Q \times K \to K$, $(q,k) \mapsto q \cdot k$, such that

1) $1 \cdot a = a$ for all $a \in K$,
2) $x \cdot (y \cdot a) = (xy) \cdot a$ for all $x, y \in Q$ and $a \in K$,
3) $x \cdot 1 = 1$ for all $x \in Q$, and
4) $x \cdot (ab) = (x \cdot a)(x \cdot b)$ for all $x \in Q$ and $a, b \in K$,

For example, if K is a normal subgroup of G, then G acts by automorphisms on K by conjugation.

Definition 7.1. Let Q and K be groups, where Q acts by automorphisms on K. A map $\varphi\colon Q \to K$ is said to be a **1-cocycle** if

$$\varphi(xy) = \varphi(x)(x \cdot \varphi(y))$$

for all $x, y \in Q$.

Let Q and K be groups, where Q acts by automorphisms on K. The set of 1-cocycles $Q \to K$ will be denoted by

$$Z^1(Q,K) = \{\delta\colon Q \to K : \delta \text{ is a 1-cocycle}\}.$$

Example 7.2. Let Q be a group acting by automorphisms on K. The semidirect product $K \rtimes Q$ is a group G that contains a normal subgroup isomorphic to K and a subgroup isomorphic to such that $G = KQ$ and $K \cap Q = \{1\}$. Under the obvious identifications, Q acts on K by conjugation. For each $k \in K$, the map $Q \to K$, $x \mapsto [k,x] = kxk^{-1}x^{-1}$, is a 1-cocycle.

Exercise 7.3. Let $\varphi\colon Q \to K$ be a 1-cocycle. Prove the following statements:
1) $\varphi(1) = 1$.
2) $\varphi(y^{-1}) = (y^{-1} \cdot \phi(y))^{-1} = y^{-1} \cdot \phi(y)^{-1}$.
3) The set $\ker\varphi = \{x \in Q : \varphi(x) = 1\}$ is a subgroup of Q.

Lemma 7.4. *Let G be a group with a normal subgroup N. If $\varphi\colon G \to N$ is a 1-cocycle (where G acts on N by conjugation) with kernel*

$$K = \ker\varphi = \{g \in G : \varphi(g) = 1\},$$

then $\varphi(x) = \varphi(y)$ if and only if $xK = yK$. In particular, $(G:K) = |\varphi(G)|$.

Proof. If $\varphi(x) = \varphi(y)$, then, since

$$\varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1} \cdot \varphi(y)) = \varphi(x^{-1})(x^{-1} \cdot \varphi(x)) = \varphi(x^{-1}x) = \varphi(1) = 1,$$

we obtain that $xK = yK$. Conversely, if $x^{-1}y \in K$, then, since

$$1 = \varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1} \cdot \varphi(y)),$$

we obtain that $\varphi(y) = x \cdot \varphi(x^{-1})^{-1}$. We conclude that $\varphi(x) = \varphi(y)$.

The second claim now is clear, as φ is constant in each coclass of K and takes $(G:K)$ different values. □

Lemma 7.5. *Let G be a finite group, N be an abelian normal subgroup of G and S, T and U be transversals of N in G. Let*

$$d(S,T) = \prod st^{-1} \in N,$$

where the product runs over all elements $s \in S$ and $t \in T$ such that $sN = tN$. The following statements hold:

1) $d(S,T)d(T,U) = d(S,U)$.
2) $d(gS,gT) = gd(S,T)g^{-1}$ *for all* $g \in G$.
3) $d(nS,S) = n^{(G:N)}$ *for all* $n \in N$.

Proof. If $s \in S$, $t \in T$ and $u \in U$ are such that $sN = tN = uN$, then, since N is abelian and $(st^{-1})(tu^{-1}) = su^{-1}$, we obtain that

$$d(S,T)d(T,U) = \prod (st^{-1})(tu^{-1}) = \prod su^{-1} = d(S,U).$$

Since $sN = tN$ if and only if $gsN = gtN$ for all $g \in G$,

$$g\left(\prod st^{-1}\right)g^{-1} = \prod gst^{-1}g^{-1} = \prod (gs)(gt)^{-1} = d(gS,gT).$$

Finally, since N is normal in G, $nsN = sN$ for all $n \in N$. Thus

$$d(nS,S) = \prod (ns)s^{-1} = n^{(G:N)}. \qquad \square$$

Recall that a subgroup K of G admits a **complement** Q if G factorizes as $G = KQ$ with $K \cap Q = \{1\}$. A typical example is the semidirect product $G = K \rtimes Q$, where K is a normal subgroup of G and Q is a subgroup of G such that $K \cap Q = \{1\}$.

Exercise 7.6. Let Q act by automorphisms on K. Prove that there is a bijection between the set of complements of K in $K \rtimes Q$ and the set $Z^1(Q,K)$.

We are now ready to prove the first version of the Schur–Zassenhaus theorem.

Theorem 7.7 (Schur–Zassenhaus). *Let G be a finite group and N be an abelian normal subgroup of G. If $|N|$ and $(G:N)$ are coprime, then N admits a complement in G. Moreover, all complements of N are conjugate.*

Proof. Let T be a transversal of N in G and $\theta\colon G \to N$, $\theta(g) = d(gT,T)$. Since N is abelian, Lemma 7.5 implies that θ is a 1-cocycle, where G acts on N by conjugation:

$$\begin{aligned}\theta(xy) &= d(xyT,T) = d(xyT,xT)d(xT,T)\\ &= (xd(yT,T)x^{-1})d(xT,T) = (x\cdot\theta(y))\theta(x).\end{aligned}$$

Claim. $\theta|_N\colon N \to N$ is surjective.

If $n \in N$, Lemma 7.5 implies that $\theta(n) = d(nT,T) = n^{(G:N)}$. Since $|N|$ and $(G:N)$ are coprime, there exist $r,s \in \mathbb{Z}$ such that $r|N| + s(G:N) = 1$. Thus

$$n = n^{r|N|+s(G:N)} = (n^s)^{(G:N)} = \theta(n^s).$$

Let $H = \ker\theta$. We prove that H is a complement of N. By Exercise 7.3, H is a subgroup of G. By Lemma 7.4,

$$|N| = |\theta(G)| = (G:H) = \frac{|G|}{|H|}.$$

Since $N \cap H$ is a subgroup of N and a subgroup of H, $N \cap H = \{1\}$, as the numbers $|N|$ and $(G:N) = |H|$ are coprime. Since $|NH| = |N||H| = |G|$, we conclude that $G = NH$. Hence H is a complement of N.

We now prove that two complements of N are conjugate. Let K be a complement of N in G. Since $NK = G$ and $N \cap K = \{1\}$, K is a transversal of N. Let $m = d(T,K) \in N$. Since the restriction map $\theta|_N$ is surjective, there exists $n \in N$ such that $\theta(n) = m$. By Lemma 7.5,

$$kmk^{-1} = kd(T,K)k^{-1} = d(kT,kK) = d(kT,K) = d(kT,T)d(T,K) = \theta(k)m$$

for all $k \in K$. Since N is abelian, $\theta(n^{-1}) = m^{-1}$. Thus

$$\begin{aligned}\theta(nkn^{-1}) &= \theta(n)n\theta(kn^{-1})n^{-1} = m\theta(kn^{-1}) \\ &= m\theta(k)k\theta(n^{-1})k^{-1} = m\theta(k)km^{-1}k^{-1} = 1.\end{aligned}$$

Therefore $nKn^{-1} \subseteq H = \ker\theta$. Since $|K| = (G:N) = |H|$, we conclude that $nKn^{-1} = H$. □

THEOREM 7.8 (Schur–Zassenhaus). *Let G be a finite group and N be a normal subgroup of G. If $|N|$ and $(G:N)$ are coprime, then N admits a complement in G.*

PROOF. We proceed by induction on $|G|$. If there is a proper subgroup K of G such that $NK = G$, then, since $(K : K \cap N) = (G : N)$ and $|N|$ are coprime, $(K : K \cap N) = (G : N)$ is coprime with $|K \cap N|$. Since $K \cap N$ is normal in K, the inductive hypothesis implies that $K \cap N$ admits a complement in K. Thus there exists a subgroup H of K such that $|H| = (K : K \cap N) = (G : N)$.

Assume that there is no proper subgroup K of G such that $NK = G$. We may assume that $N \neq \{1\}$ (otherwise, G would be a complement of N in G). Since N is contained in every maximal subgroup of G (because, if there is a maximal subgroup $M \subsetneq G$ such that $N \not\subseteq M$, then $NM = G$), it follows that $N \subseteq \Phi(G)$. By Frattini's theorem 4.33, $\Phi(G)$ is nilpotent. Thus N is nilpotent and then $Z(N) \neq \{1\}$. Let $\pi\colon G \to G/Z(N)$ be the canonical map. Since N is normal in G and $Z(N)$ is characteristic in N, $Z(N)$ is normal in G. Moreover,

$$(\pi(G) : \pi(N)) = \frac{|\pi(G)|}{|\pi(N)|} = \frac{|G/Z(N)|}{|N/N \cap Z(N)|} = (G : N)$$

is coprime with $|N|$. Then $(\pi(G) : \pi(N))$ is coprime with $|\pi(N)|$. By the inductive hypothesis, $\pi(N)$ admits a complement in $G/Z(N)$, say $\pi(K)$ for some subgroup K of G. Hence $G = NK$, as $\pi(G) = \pi(N)\pi(K) = \pi(NK)$. Since $K = G$ (because there is no K such that $G = NK$), $\pi(N)$ is abelian, as

$$\pi(Z(N)) = \pi(N) \cap \pi(K) = \pi(N) \cap \pi(G) = \pi(N).$$

Thus $N \subseteq Z(N)$ is abelian. By Theorem 7.7, the subgroup N admits a complement. □

THEOREM 7.9 (Schur–Zassenhaus conjugation theorem). *Let G be a finite group and N be a normal subgroup of G such that $|N|$ and $(G:N)$ are coprime. If either N or G/N is solvable, then all complements of N in G are conjugate.*

PROOF. Let G be a minimal counterexample to the theorem, that is there are complements K_1 and K_2 of N in G such that K_1 and K_2 are not conjugate.

CLAIM. Every subgroup U of G satisfies the assumptions of the theorem with respect to the normal subgroup $U \cap N$.

Since N is normal in G, $U \cap N$ is normal in U. Moreover, $|U \cap N|$ and $(U : U \cap N)$ are coprime, as $|U \cap N|$ divides $|N|$ and $(U : U \cap N) = (UN : N)$ divides $(G : N)$. If G/N is solvable, then $U/U \cap N$ is solvable, as $U/U \cap N$ is isomorphic to a subgroup of G/N. If N is solvable, then so is $U \cap N$.

CLAIM. If there is a normal subgroup L of G such that $\pi(N)$ is normal in $\pi(G)$, where $\pi\colon G \to G/L$ is the canonical map, then $\pi(G)$ satisfies the theorem's assumptions with respect to $\pi(N)$. In this case, if H is a complement of N in G, then $\pi(H)$ is a complement of $\pi(N)$ in $\pi(G)$.

If N is solvable, then so is $\pi(N)$. If G/N is solvable, then so is $\pi(G)/\pi(N) \simeq G/NL$. Moreover, $(\pi(G) : \pi(N)) = \frac{|G/L|}{|N/N\cap L|}$ divides $(G : N)$.

If H is a complement of N in G, $|\pi(H)|$ and $|\pi(N)|$ are coprime. Then $\pi(H)$ is a complement of $\pi(N)$, as $\pi(G) = \pi(N)\pi(H) = \pi(NH)$ and $\pi(N) \cap \pi(H) = \{1\}$.

CLAIM. N is minimal normal in G.

Let $M \neq \{1\}$ be a normal subgroup of G such that $M \subseteq N$. Let $\pi\colon G \to G/M$ be the canonical map. Then $\pi(G)$ satisfies the theorem's assumptions with respect to the normal subgroup $\pi(N)$. By the minimality of $|G|$, there exists $x \in G$ such that $\pi(xK_1x^{-1}) = \pi(K_2)$. The subgroup $U = MK_2$ satisfies the theorem's assumptions with respect to the normal subgroup $U \cap N$ of U. Since $xK_1x^{-1} \cup K_2 \subseteq U$, we conclude that both xK_1x^{-1} and K_2 complement $U \cap N$ in U. Hence $MK_2 = G$, as xK_1x^{-1} and K_2 are not conjugate and G, as G is a minimal counterexample. Therefore $M = N$, as

$$\frac{|K_2|}{|M \cap K_2|} = (MK_2 : M) = (G : M) = \frac{|NK_2|}{|M|} = (N : M)|K_2|.$$

CLAIM. N is not solvable and G/N is solvable.

Otherwise, by Lemma 1.22, N is abelian (because it is minimal normal). This contradicts Theorem 7.7, as it states that K_1 and K_2 are conjugate.

Let $p\colon G \to G/N$ be the canonical map and S be a subgroup such that $p(S)$ is minimal normal in $p(G) = G/N$. By Lemma 1.22, $p(S)$ is a p-group for some prime number p. Since $G = NK_1 = NK_2$ and $N \subseteq S$, Dedekind's lemma 4.28 implies that

$$S = N(S \cap K_1) = N(S \cap K_2).$$

Hence both $S \cap K_1$ and $S \cap K_2$ complement N in S. Since $p(S) = p(S \cap K_1) = p(S \cap K_2)$ is a p-group, p divides $|S|$. The theorem's assumptions hold for S with respect to the normal subgroup N, so $|N|$ and $(S : N)$ are coprime. If $p \mid |N|$, then $p \nmid (S : N) = |S \cap K_1| = |S \cap K_2|$, a contradiction. Thus $p \nmid |N|$ and hence $p \nmid |S|$. This implies that both $S \cap K_1$ and $S \cap K_2$ are Sylow p-subgroups of S, as

$$|S \cap K_1| = (S : N) = |S \cap K_2|.$$

By Sylow's theorem, there exists $s \in S$ such that

$$S \cap sK_1s^{-1} = S \cap K_2.$$

In particular, $S \neq G$ by the minimality of G. Let

$$L = S \cap K_2 = S \cap sK_1s^{-1} \neq \{1\}.$$

Since S is normal in G, $sK_1s^{-1} \cup K_2 \subseteq N_G(L)$ (because L is both normal in sK_1s^{-1} and in K_2). The subgroups $sK_1s^{-1} \subseteq N_G(L)$ and $K_2 \subseteq N_G(L)$ complement $N \cap N_G(L)$ in $N_G(L)$. Hence $N_G(L) = G$ by the minimality of G (if $N_G(L) \neq G$, then both sK_1s^{-1} and K_2 are conjugate in G because they are conjugate in $N_G(L)$). Therefore L is normal in G.

Let $\pi_L\colon G \to G/L$ be the canonical map. Since both $\pi_L(K_1)$ and $\pi_L(K_2)$ complement $\pi_L(N)$ in $\pi_L(G)$, the minimality of $|G|$ implies that there exists $g \in G$ such that $\pi_L(gK_1g^{-1}) = \pi_L(K_2)$, that is there exists $g \in G$ such that $(gK_1g^{-1})L = K_2L$. Hence $gK_1g^{-1} \cup K_2 \subseteq \langle K_2, L\rangle = K_2$, because $L \subseteq K_2$. In conclusion, $gK_1g^{-1} = K_2$, a contradiction to the minimality of $|G|$. □

By the Feit–Thompson theorem, in the previous theorem, we do not need to assume that either N or G/N is solvable. Since every group of odd order is solvable and $|N|$ and $(G:N)$ are coprime, one of these groups should have odd order.

Lecture 8. 18/04/2024

THEOREM 8.1. *Let G be a finite solvable group and p a prime number dividing $|G|$. There exists a maximal subgroup M of G of index a power of p.*

PROOF. We proceed by induction on $|G|$. If G is a p-group, the result clearly holds. So we may assume that $|G|$ is divisible by at least two different prime numbers. Let p be a prime dividing $|G|$, N be a minimal normal subgroup of G and $\pi\colon G \to G/N$ be the canonical map. Since G is solvable, by Lemma 1.22, N is a q-group for some prime q. Since G/N is solvable, if p divides $(G:N)$, then, by the inductive hypothesis, G/N has a maximal subgroup M_1 of index a power of p. By the correspondence theorem, $M = \pi^{-1}(M_1)$ is a maximal subgroup of G of index a power of p. p. If p does not divide $(G:N)$, then p divides $|N|$. Thus $N \in \mathrm{Syl}_p(G)$. Since N is normal in G and $|N|$ and $|G/N|$ are coprime, by Schur–Zassenhaus theorem 7.8, there exists a complement K of N in G, that is $G = NK$ and $N \cap K = \{1\}$. Let M be a maximal subgroup containing K. Then $(G:M)$ is a power of p. □

We now discuss an application to finite super-solvable groups.

DEFINITION 8.2. A finite group G is said to be **lagrangian** if for each d dividing $|G|$ there exists a subgroup of G of order d.

The group $\mathbb{A}_4$ is not lagrangian, as it has no subgroups of order six.

THEOREM 8.3. *Every finite super-solvable group is lagrangian.*

PROOF. Let p be a prime number dividing $|G|$. Since subgroups of super-solvable groups are super-solvable, it is enough to show that there exists a subgroup of index p. Since G is solvable, there exists a maxima subgroup M of index p^α by Theorem 8.1. Since maximal subgroups of super-solvable groups have prime index by Theorem 6.11, we conclude that $\alpha = 1$. □

See [**8**] for an elementary proof.

§ 8.1. *Hall's theory for solvable groups. As an application of the Schur–Zassenhaus theorem, we present Hall's theory of solvable groups. For an elementary presentation, see [**21**].

DEFINITION 8.4. Let G be a finite group and π be a set of prime numbers. We say that G is a **π-group** if every prime dividing $|G|$ belongs to π. Similarly, a π-subgroup of G is a subgroup of G that is also a π-group.

For a set π of prime numbers, we define a π-number as an integer whose prime divisors belong to π. The set of prime numbers not belonging to π will be denoted as π'. Thus a π'-number is an integers not divisible by the prime numbers of π.

DEFINITION 8.5. Let G be a group and π be a set of prime numbers. A subgroup H of G is a **Hall π-subgroup** if H is a π-subgroup of G and $(G:H)$ is a π'-number.

We now prove that a finite solvable group of order nm with $\gcd(n,m) = 1$ always admits a subgroup of order m.

THEOREM 8.6 (Hall's!existence theorem). *Let π be a set of prime numbers and G be a finite solvable group. Then G has a Hall π-subgroup.*

PROOF. Assume that $|G| = nm > 1$ and $\gcd(n,m) = 1$. We want to show that G admits a subgroup of order m. We proceed by induction on $|G|$. Let K be a minimal normal subgroup of G and $\pi\colon G \to G/N$ be the canonical map. Since G is solvable, K is a p-group (Lemma 1.22).

There are two cases to consider. Assume first that p divides m. Since $|G/K| < |G|$, the inductive hypothesis and the correspondence theorem imply that there exists a subgroup J of G containing K such that $\pi(J)$ is a subgroup of $\pi(G) = G/K$ of order $m/|K|$. Then J has order m, as

$$m/|K| = |\pi(J)| = \frac{|J|}{|K \cap J|} = (J : K).$$

Assume now that p does not divide m. By the inductive hypothesis and the correspondence theorem, there exists a subgroup H of G containing K such that $\pi(H)$ is a subgroup of G/K of order m. Since $|H| = m|K|$, K is normal in H and $|K|$ is coprime with $|H : K|$, the Schur–Zassenhaus theorem (Theorem 7.8) implies that there exists a complement J of K in H. Hence J is a subgroup of G such that $|J| = m$. □

EXAMPLE 8.7. The group $\mathbb{A}_5$ contains a Hall $\{2,3\}$-subgroups isomorphic to $\mathbb{A}_4$.

EXAMPLE 8.8. The simple group $\mathbf{PSL}_3(2)$ of order 168 does not contain Hall $\{2,7\}$-subgroups.

THEOREM 8.9 (Hall's conjugation theorem). *Let G be a finite solvable group and π be a set of prime numbers. Then all two Hall π-subgroups of G are conjugate.*

PROOF. We may assume that $G \neq \{1\}$. We proceed by induction on $|G|$. Let H and K be Hall π-subgroups of G. Let M be a minimal normal subgroup of G and $\pi\colon G \to G/M$ be the canonical map. Since G is solvable, M is a p-group for some prime number p (Lemma 1.22). Since $\pi(H)$ and $\pi(K)$ are both Hall π-subgroups of G/M, by the inductive hypothesis, the subgroups $\pi(H)$ and $\pi(K)$ are conjugate in G/M. Thus there exists $g \in G$ such that $gHMg^{-1} = KM$.

There are two cases to consider. Assume first that $p \in \pi$. Since $|HM|$ and $|KM|$ are π-numbers and $|H| = |K|$ is the largest π-number dividing $|G|$, we conclude that $H = HM$ and $K = KM$. In particular, $gHg^{-1} = K$.

Assume now that $p \notin \pi$. Then K admits a complement M in KM, as $K \cap M = \{1\}$. We claim that gHg^{-1} complements M in KM. Since M is normal in G,

$$(gHg^{-1})M = gHMg^{-1} = KM,$$

and $gHg^{-1} \cap M = \{1\}$, as $p \notin \pi$. These complements are conjugate by the Schur–Zassenhaus theorem 7.9. □

COROLLARY 8.10. *Let G be a finite group, N a normal subgroup of G and $n = |N|$. Assume that either N of G/N is solvable. If $|G : N| = m$ is coprime with n and m_1 divide a m, then every subgroup of G of order m_1 is contained in some subgroup of order m.*

PROOF. Let H be a complement of N in G. Then $|H| = m$. Let H_1 be a subgroup of G such that $|H_1| = m_1$. Since $\gcd(n,m) = 1$, $m_1 = |H_1| = |H \cap NH_1|$, as

$$\frac{|H||N||H_1|}{|H \cap NH_1|} = \frac{|H||NH_1|}{|H \cap NH_1|} = |H(NH_1)| = |G| = |NH| = |N||H|.$$

Since both H_1 and $H \cap NH_1$ are complements of N in NH_1, and both groups have orders coprime with n, there exists $g \in G$ such that $H_1 = g(H \cap NH_1)g^{-1}$. Thus $H_1 \subseteq gHg^{-1}$ and hence $|gHg^{-1}| = m$. □

§ 8.2. Subnormality.

DEFINITION 8.11. Let G be a group. A subgroup H of G is said to be subnormal in G if there is a sequence of subgroups

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G$$

with H_i normal in H_{i+1} for all $i \in \{0, \ldots, k-1\}$.

EXAMPLE 8.12. Let $G = \mathbb{S}_4$. Then $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ is normal in G. The subgroup $L = \{\mathrm{id}, (12)(34)\}$ is subnormal in G (and not normal). es subnormal.

EXERCISE 8.13. Prove that the correspondence theorem preserves subnormality.

THEOREM 8.14. *Let G be a finite group. Then G is nilpotent if and only if every subgroup of G is subnormal in G.*

PROOF. Assume first that every subgroup of G is subnormal in G. Let H be a subnormal subgroup of G, where

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G$$

with H_i normal in H_{i+1}. Without loss of generality, we may assume that $H \subsetneq H_1$. Since $H \subsetneq H_1 \subseteq N_G(H)$, G is nilpotent by Exercise 4.4.

Assume now that G is nilpotent. Let H be a subgroup of G. We proceed by induction on $(G : H)$. If $(G : H) = 1$, then $H = G$ and the theorem holds. If $H \neq G$, since $H \subsetneq N_G(H)$ by Lemma 2.26,

$$(G : N_G(H)) < (G : H).$$

By the inductive hypothesis, $N_G(H)$ is subnormal in G. Since H is normal in $N_G(H)$, we conclude that H is subnormal in G. □

COROLLARY 8.15. *Let G be a group and K be a central subgroup of G (that is, $K \subseteq Z(G)$). Then G is nilpotent if and only if G/K is nilpotent.*

PROOF. If G is nilpotent, then so is G/K. Conversely, let $\pi\colon G \to G/K$ be the canonical map and U be a subgroup of G. Since G/K is nilpotent, Theorem 8.14 implies that $\pi(U)$ is a subnormal subgroup of G/K. By the correspondence theorem, UK is a subnormal subgroup of G. Since K is central, U is normal in UZ. Hence U is subnormal in G and therefore G is nilpotent by Theorem 8.14. □

THEOREM 8.16. *Let G be a finite group and H be a subgroup of G. Then H is nilpotent and subnormal in G if and only if $H \subseteq F(G)$.*

PROOF. Assume first that $H \subseteq F(G)$. Since $F(G)$ is nilpotent by Theorem 5.12, so is H. Moreover, since H is subnormal in $F(G)$ (Theorem 8.14) and $F(G)$ is normal in G, H is subnormal in G.

Assume now that H is nilpotent and subnormal in G. We proceed by induction on $|G|$. If $H = G$, then the result holds. Assume then that $H \neq G$. Since H is subnormal in G, there is a sequence

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G$$

of subgroups of G with H_i normal in H_{i+1} for all i. Let $M = H_{k-1}$. Since $M \neq G$ and M is normal in G, $H \subseteq F(M)$ by the inductive hypothesis. Thus $H \subseteq F(M) = M \cap F(G) \subseteq F(G)$ by Corollary 5.15. □

Before proving another important theorem of Wielandt, we need a lemma.

LEMMA 8.17. *Let M and N be normal subgroups of G such that $M \cap N = \{1\}$. Then $M \subseteq C_G(N)$.*

PROOF. Let $m \in M$ and $n \in N$. Then $[n,m] = (nmn^{-1})m \in M$, since M is normal in G and Moreover, $[n,m] = n(mn^{-1}m^{-1}) \in N$, since N is normal in G. Thus $[n,m] \in M \cap N = \{1\}$. □

EXERCISE 8.18. A group G is said to be **characteristically simple** if G is non-trivial and has no proper characteristic subgroups. Prove that any minimal normal subgroup of G is characteristically simple.

DEFINITION 8.19. Let G be a group. If G admits minimal normal subgroups, the **socle** of G is defined as the subgroup $\mathrm{Soc}(G)$ of G generated by all minimal normal subgroups of G. If G admits no minimal normal subgroups, then $\mathrm{Soc}(G) = \{1\}$.

For example, $\mathrm{Soc}(\mathbb{Z}) = \{0\}$ and $\mathrm{Soc}(\mathbf{SL}_2(3)) \simeq C_2$.

EXERCISE 8.20. Prove that the socle of a group is a direct product of minimal normal subgroups.

EXERCISE 8.21. Prove the following statements:

1) A direct product of isomorphic simple groups is characteristically simple.

2) A characteristically simple group with at least one minimal normal subgroup is a direct product of isomorphic simple groups.

THEOREM 8.22 (Wielandt). *Let G be a finite group. If S is a subnormal group of G and M is a minimal normal subgroup of G, then $M \subseteq N_G(S)$.*

PROOF. We proceed by induction on $|G|$. If $S = G$ the result holds. So assume that $S \neq G$. Since S is subnormal in G, there exists a sequence

$$S = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_{k-1} \subseteq S_k = G$$

of subgroups of G such that S_i is normal in S_{i+1} for all i. Let $N = S_{k-1}$.

If $M \cap N \neq \{1\}$, then $M \subseteq N$ (because since M and N are both normal in G, $M \cap N = M$ by the minimality of M). We claim that $M \subseteq \mathrm{Soc}(N)$. Since $M \neq \{1\}$ and M is normal in N, $M \cap \mathrm{Soc}(N) \neq \{1\}$. Moreover, since $\mathrm{Soc}(N)$ is characteristic in N and N is normal in G, it follows that $\mathrm{Soc}(N)$ is normal in G. Hence $M \cap \mathrm{Soc}(N)$ is a normal subgroup of G. Since $\{1\} \neq M \cap \mathrm{Soc}(N) \subseteq M$, we conclude that $M \cap \mathrm{Soc}(N) = M$ by the minimality of M. By the inductive hypothesis, every minimal normal subgroup of N normalizes S. Thus $\mathrm{Soc}(N) \subseteq N_N(S) \subseteq N_G(S)$ and therefore

$$M \subseteq \mathrm{Soc}(N) \subseteq N_G(S).$$

If $M \cap N = 1$, Lemma 8.17 implies that

$$M \subseteq C_G(N) \subseteq C_G(S) \subseteq N_G(S).$$ □

COROLLARY 8.23. *Let G be a finite group and S be a subnormal subgroup of G. Then*

$$\mathrm{Soc}(G) \subseteq N_G(S).$$

PROOF. By Theorem 8.22, every minimal normal subgroup of G is contained in $N_G(S)$. Then $\mathrm{Soc}(G) = \langle M : M \text{ minimal normal subgroup of } G \rangle \subseteq N_G(S)$. □

THEOREM 8.24 (Wielandt). *Let G be a finite group and S and T be subnormal subgroups of G. Then $S \cap T$ and $\langle S, T\rangle$ are subnormal in G.*

PROOF. We first prove that $S \cap T$ is subnormal in G. Since subnormality is a transitive relation, it is enough to see that $S \cap T$ is subnormal in T. Since S is subnormal in G, there exists a sequence

$$S = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_k = G$$

of subgroups of G such that S_i is normal in S_{i+1} for all i. Each $S_{j-1} \cap T$ is normal in $S_j \cap T$. Then $S \cap T$ is subnormal in T.

We now prove that $\langle S, T\rangle$ is subnormal in G We proceed by induction on $|G|$. Assume that $G \neq \{1\}$. Let M be a minimal normal subgroup of G and $\pi\colon G \to G/M$ be the canonical map. Since both $\pi(S)$ and $\pi(T)$ subnormal in G/M and $|G/M| < |G|$, the inductive hypothesis implies that

$$\pi(\langle S, T\rangle M) = \pi(\langle S, T\rangle) = \langle \pi(S), \pi(T)\rangle$$

is subnormal in G/M. By the correspondence theorem, $\langle S, T\rangle M$ is subnormal in G. Theorem 8.22 implies that $M \subseteq N_G(S)$ and $M \subseteq N_G(T)$. Hence $M \subseteq N_G(\langle S, T\rangle)$. Since $\langle S, T\rangle$ is normal in $\langle S, T\rangle M$ and $\langle S, T\rangle M$ is subnormal in G, we conclude that $\langle S, T\rangle$ is subnormal in G. □

§ 8.3. Wielandt's zipper theorem.

THEOREM 8.25 (Wielandt). *Let G be a finite group and S be a subgroup of G subnormal in every proper subgroup of G containing S. If S is not subnormal in G, then there exists a unique maximal subgroup of G containing S.*

PROOF. We proceed by induction on $(G : S)$. If S is not subnormal in G, then $S \neq G$ and the case where $(G : S) = 1$ holds.

Since S is not subnormal in G, $N_G(S) \neq G$. Then $S \subseteq N_G(S) \subseteq M$ for some maximal subgroup M of G. Assume that $S \subseteq K$ for some maximal subgroup K of G. We claim that que $K = M$. Since $S \subseteq K \neq G$, S is subnormal in K. If S is normal in K, then $K \subseteq N_G(S) \subseteq M$. Hence $K = M$ by the maximality of K. If S is not normal in K, there exist a sequence $S_0, \ldots, S_m$ of subgroups of K such that

$$S = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_m = K,$$

where S_i is normal in S_{i+1} for all i and S is not normal in S_2. Let $x \in S_2$ be such that $xSx^{-1} \neq S$ and $T = \langle S, xSx^{-1}\rangle \subseteq K$.

Since $xSx^{-1} \subseteq xS_1x^{-1} = S_1 \subseteq N_G(S)$, we obtain that $T \subseteq N_G(S) \subseteq M$. Moreover, S is normal in T. Thus $T \neq G$.

We claim that T satisfies the theorem's assumptions. If T is subnormal in G, then, since S is normal in T, S is subnormal in G. If H is a proper subgroup of G containing T, then, since $S \subseteq H$, S is subnormal in H. Moreover, xSx^{-1} is subnormal in H. Hence T is subnormal in H by Theorem 8.24.

Since $S \subsetneq T$, $(G : T) < (G : S)$. By the inductive hypothesis, T is contained in a unique maximal subgroup of G. Therefore $K = M$, since $T \subseteq M$ and $T \subseteq K$. □

Before giving an application, we need a lemma.

LEMMA 8.26. *Let G be a group and H be a subgroup of G. If $(xHx^{-1})H = G$ for some $x \in G$, then $H = G$.*

PROOF. Write $x = uv$ for some $u \in xHx^{-1}$ and $v \in H$. Since $u \in xHx^{-1}$ and $u^{-1}x = v \in H$, we obtain that $H = vHv^{-1} = u^{-1}(xHx^{-1})u = xHx^{-1}$. Thus $G = H$. □

Recall that two subgroups S and T of a group G are said to be **permutable** if $ST = TS$.

THEOREM 8.27. *Let G be a finite group and S be a subgroup of G permutable with any of its conjugates. Then S is subnormal in G.*

PROOF. We proceed by induction on $|G|$. Assume that S is subnormal in every subgroup H such that $S \subseteq H \subsetneq G$. If S is not subnormal in G, then, by Theorem 8.25, there exists a unique maximal subgroup M of G such that $S \subseteq M$. Let $x \in G$ and $T = xSx^{-1}$. By Lemma 8.26, $ST \neq G$ (because $S \neq G$). Thus ST is contained in some maximal subgroup of G. Since $S \subseteq ST$ and S is contained in a unique maximal subgroup of G, we conclude that $T \subseteq ST \subseteq M$. Since $S^G = \langle xSx^{-1} : x \in G\rangle \subseteq M \neq G$, the inductive hypothesis implies that S is subnormal in S^G. Hence S is subnormal in G since S^G is normal in G, a contradiction. □

§ 8.4. Baer's theorem.

THEOREM 8.28 (Baer). *Let G be a finite group and H be a subgroup of G. Then $H \subseteq F(G)$ if and only if $\langle H, xHx^{-1}\rangle$ is nilpotent for all $x \in G$.*

PROOF. If $H \subseteq F(G)$, then $xHx^{-1} \subseteq F(G)$ for all $x \in G$, since $F(G)$ is normal in G. Thus $\langle H, xHx^{-1}\rangle$ is nilpotent, as it is a subgroup of $F(G)$.

Conversely, assume that $\langle H, xHx^{-1}\rangle$ is nilpotent for all $x \in G$. Since $H \subseteq \langle H, xHx^{-1}\rangle$, H is nilpotent. By Theorem 8.16, it is enough to see that H is subnormal in G. We proceed by induction on $|G|$. Suppose that H is not subnormal in G. If H is properly contained in some subgroup K, then, since $\langle H, kHk^{-1}\rangle$ is nilpotent for all $k \in K$, H is subnormal in K by the inductive hypothesis. By Theorem 8.25, there exists a unique maximal subgroup M of G containing H. There are two cases to consider.

Assume first that $G = \langle H, xHx^{-1}\rangle$ for some $x \in G$. Since G is nilpotent, H subnormal in G by Theorem 8.14, a contradiction.

Assume now that $\langle H, xHx^{-1}\rangle \neq G$ for all $x \in G$. For each $x \in G$, there exists a maximal subgroup containing $\langle H, xHx^{-1}\rangle$. Since $H \subseteq \langle H, xHx^{-1}\rangle$ and H is contained in a unique maximal subgroup, we conclude that $\langle H, xHx^{-1}\rangle \subseteq M$ for all $x \in G$. In particular, the normal closure H^G of H is properly contained in G. By the inductive hypothesis, H is subnormal in H^G and H^G is normal in G, we conclude that H is subnormal in G, a contradiction. □

§ 8.5. Zenkov's theorem.

THEOREM 8.29 (Zenkov). *Let G be a finite group and A and B be abelian subgroups of G. Let $M \in \{A \cap gBg^{-1} : g \in G\}$ such that no $A \cap gBg^{-1}$ is properly contained in M. Then $M \subseteq F(G)$.*

PROOF. Without loss of generality, we may assume that $M = A \cap B$. Using induction on $|G|$, we prove that $M \subseteq F(G)$.

Assume first that $G = \langle A, gBg^{-1}\rangle$ for some $g \in G$. Since A and B are both abelian,

$$A \cap gBg^{-1} \subseteq Z(G)$$

and hence

$$A \cap gBg^{-1} = g^{-1}(A \cap gBg^{-1})g \subseteq A \cap B = M.$$

By the minimality of M,

$$M = A \cap gBg^{-1} \subseteq Z(G) \subseteq F(G)$$

by Corollary 5.13.

Assume now that $G \neq \langle A, gBg^{-1}\rangle$ for all $g \in G$. Let $g \in G$, $H = \langle A, gBg^{-1}\rangle \neq G$ and $C = B \cap H$. Since $A \subseteq H$, we obtain that $M = A \cap B = A \cap C$ and $A \cap hCh^{-1} = A \cap hBh^{-1}$ for all $h \in H$. This implies that no $A \cap hCh^{-1}$ is properly contained in $A \cap C$. By the inductive hypothesis on H,

$$M = A \cap B = A \cap C \subseteq F(H).$$

We now prove that every Sylow p-subgroup P of M is contained in $F(G)$. Since M is generated by its Sylow subgroups, $M \subseteq F(G)$. If $P \in \mathrm{Syl}_p(M)$, then $P \subseteq M \subseteq F(H)$. Since $O_p(H)$ is the only Sylow p-subgroup of $F(H)$, $P \subseteq O_p(H)$. Since $P \subseteq M \subseteq B$,

$$gPg^{-1} \subseteq gBg^{-1} \subseteq H$$

for all $g \in G$. Thus $O_p(H)(gPg^{-1})$ is a p-subgroup of H containing $\langle P, gPg^{-1}\rangle$. Hence $\langle P, gPg^{-1}\rangle$ is nilpotent for all $g \in G$, since it is a p-group. By Baer's theorem 8.28, $P \subseteq F(G)$ for all Sylow p-subgroup P of M. □

Corollary 8.30. *Let G be a non-trivial finite group and A be an abelian subgroup of G such that $|A| \geq (G : A)$. Then $A \cap F(G) \neq \{1\}$.*

Proof. Let $g \in G$. We may assume that $G \neq A$. Then $(gAg^{-1})A \neq G$ by Lemma 8.26. Since $|gAg^{-1}||A| = |A|^2 \geq |A|(G : A) = |G|$,

$$|G| > |gAg^{-1}A| = \frac{|A||gAg^{-1}|}{|A \cap gAg^{-1}|} \geq \frac{|G|}{|A \cap gAg^{-1}|}.$$

Hence $A \cap gAg^{-1} \neq 1$ for all $g \in G$. In particular, no $A \cap gAg^{-1}$ is properly contained in A. By Zenkov's theorem 8.29, $A \subseteq F(G)$. □

Corollary 8.31. *Let $G = NA$ be a finite group, where N is a normal subgroup of G, A is an abelian subgroup of G and $C_A(N) = \{1\}$. If $F(N) = \{1\}$, then $|A| < |N|$.*

Proof. Since N is normal in G,

$$N \cap F(G) = F(N) = \{1\}$$

by Corollary 5.15. Thus $[N, F(G)] = \{1\}$, since both N and $F(G)$ are normal in G. Since

$$|A| \geq |N| \geq \frac{|N|}{|N \cap A|} = (NA : A) = (G : A),$$

$A \cap F(G) \neq \{1\}$ by Corollary 8.30. If $1 \neq a \in A \cap F(G)$, then $a \in C_A(N) = 1$, a contradiction. □

§ 8.6. Brodkey's theorem.

Theorem 8.32 (Brodkey). *Let G be a finite group such that there exists an abelian $P \in \mathrm{Syl}_p(G)$. Then there exist $S, T \in \mathrm{Syl}_p(G)$ such that $S \cap T = O_p(G)$.*

Proof. By applying Zenkov's theorem (Theorem 8.29) with $A = B = P$,

$$P \cap gPg^{-1} \subseteq F(G)$$

for some $g \in G$. Since $O_p(G)$ is the only Sylow p-subgroup of $F(G)$, $P \cap gPg^{-1} \subseteq O_p(G)$. Hence $P \cap gPg^{-1} = P_p(G)$, since $O_p(G)$ is contained in every Sylow p-subgroup of G. □

Corollary 8.33. *Let G be a finite group. If there exists an abelian $P \in \mathrm{Syl}_p(G)$,*

$$(G : O_p(G)) \leq (G : P)^2.$$

PROOF. By Brodkey's theorem, there exist $S,T \in \mathrm{Syl}_p(G)$ such that $S \cap T = O_p(G)$. Then

$$|G| \geq |ST| = \frac{|S||T|}{|S \cap T|} = \frac{|P|^2}{|O_p(G)|},$$

which implies the claim. □

COROLLARY 8.34. *Let G be a finite group. If there exists an abelian $P \in \mathrm{Syl}_p(G)$ such that $|P| < \sqrt{|G|}$, then $O_p(G) \neq \{1\}$.*

PROOF. Since $(G:P)^2 < |G|$, the previous corollary implies that $O_p(G) \neq \{1\}$. □

§ 8.7. Lucchini's theorem.

THEOREM 8.35 (Lucchini). *Let G be a finite group and A be a proper cyclic subgroup of G. If $K = \mathrm{Core}_G(A)$, then $(A:K) < (G:A)$.*

PROOF. We proceed by induction on $|G|$. Let $\pi\colon G \to G/K$ be the canonical map. Note that $\mathrm{Core}_{G/K}\pi(A)$ is trivial.

Assume first that $K \neq \{1\}$. Since $\pi(A)$ is a proper cyclic subgroup of G/K and $K \subseteq A$, the inductive hypothesis implies that

$$(A:K) = |\pi(A)| = (\pi(A):\pi(K)) < (\pi(G):\pi(A)) = \frac{(G:K)}{(A:K)} = (G:A).$$

Assume now that $K = \{1\}$. We want to prove that $|A| < (G:A)$. Suppose that $|A| \geq (G:A)$. Since $A \neq G$, $A \cap F(G) \neq \{1\}$ by Corollary 8.30. In particular, $F(G) \neq \{1\}$. Let E be a minimal normal subgroup of such that $E \subseteq F(G)$. By Theorem 3.8, $E \cap Z(F(G)) \neq \{1\}$. Since $E \cap Z(F(G))$ is normal in G and E is minimal, $E \cap Z(F(G)) = E$, that is $E \subseteq Z(F(G))$. In particular, E is abelian. By the minimality of E, there is a prime number p such that $x^p = 1$ for all $x \in E$.

CLAIM. *$A \cap F(G)$ is a normal subgroup of EA.*

Since E is normal in G, EA is a subgroup of G. Since $A \cap F(G) \subseteq A$, $A \cap F(G)$ is a subgroup of EA. Since $F(G)$ is normal in G, $a(A \cap F(G))a^{-1} = A \cap F(G)$ for all $a \in A$. Moreover, $E \subseteq Z(F(G))$ and $A \cap F(G) \subseteq F(G)$ imply that $x(A \cap F(G))x^{-1} = A \cap F(G)$ for all $x \in E$.

CLAIM. *$EA \neq G$.*

If $G = EA$, then, since $A \cap F(G)$ is a normal subgroup of G contained in A, we conclude that $\{1\} \neq A \cap F(G) \subseteq K = 1$, a contradiction.

Let $p\colon G \to G/E$ the canonical map. By the correspondence theorem, there exists a normal subgroup M of G such that $E \subseteq M$ and $p(M) = \mathrm{Core}_{G/E}(p(A))$. Since $EA \neq G$, $p(A)$ is a proper cyclic subgroup of $p(G)$. Since $p(A) \simeq A/A \cap E \simeq EA/E$ and $p(M) \simeq M/E$, the inductive hypothesis implies that $(EA:M) < (G:EA)$, as

$$\frac{|EA/E|}{|M/E|} = (p(A):p(M)) < (p(G):p(A)) = \frac{|G/E|}{|EA/E|}.$$

CLAIM. *$MA = EA$.*

Since $E \subseteq M$, $EA \subseteq MA$. Conversely, if $m \in M$, then, since $p(m) \in \mathrm{Core}_{G/E}(p(A))$, we obtain that $p(m) \in p(A)$. Thus $m \in EA$.

Let $B = A \cap M$. Since $(AE : M) < (G : EA)$,

$$(A : B) = |A/A \cap M| = |AM/M| = (EA : M).$$

By the inductive hypothesis,

$$\begin{aligned}(M : B) &= (M : A \cap M) = (MA : A) \\ &= (EA : A) = \frac{(G : A)}{(G : EA)} < \frac{(G : A)}{(AE : M)} = \frac{(G : A)}{(A : B)} \leq |B|,\end{aligned} \tag{8.1}$$

as $|A| \geq (G : A)$.

Claim. $M = EB$.

Since $E \cup B \subseteq M$, $EB \subseteq M$. Conversely, if $m \in M$, then $m = ea$ for some $e \in E$ and $a \in A$. Since $e^{-1}m = a \in A \cap M = B$ (because $E \subseteq M$), $m \in EB$.

Claim. M is not abelian.

Suppose that M is abelian. The map $f : M \to M$, $m \mapsto m^p$, is a group homomorphism such that $E \subseteq \ker f$. Since $M = EB$, $f(M) \subseteq f(B) \subseteq B \subseteq A$. Since M is normal in G, $f(M)$ is normal in G. Thus $f(M) = \{1\}$, as $K = \mathrm{Core}_G(A) = \{1\}$ is the largest normal subgroup of G contained in A. In particular, since B is normal in $M = EB$, M/B is a p-group. Since $B \subseteq M$, $f(B) = \{1\}$. Moreover, since $B \subseteq A$ is cyclic, $|B| \leq p$. By using (8.1), $(M : B) < |B| \leq p$. This implies that $M = B \subseteq A$ and $M = E = 1$ (because M is normal in G and $\mathrm{Core}_G(A) = K = \{1\}$ is the largest normal subgroup of G containing A), a contradiction.

Claim. $Z(M)$ is cyclic.

Since M is not abelian and $M/E = EB/E \simeq B/E \cap B$ is cyclic, $E \not\subseteq Z(M)$, that is $E \cap Z(M) \subsetneq E$. Thus

$$E \cap Z(M) = \{1\} \tag{8.2}$$

by the minimality of E. Hence

$$Z(M) = Z(M)/Z(M) \cap E \simeq p(Z(M)) \subseteq p(M) = \mathrm{Core}_{G/E}\, p(A) \subseteq p(A)$$

and therefore $Z(M)$ is cyclic, since $p(A)$ is cylic.

Since $B \subseteq A$ is abelian and $(M : B) < |B|$, $B \cap F(M) \neq 1$ by Corollary 8.30. Then $[E, F(M)] = 1$ (because $E \subseteq Z(F(G))$ and $F(M) \subseteq F(G)$ by Corollary 5.15). Hence $B \cap F(M) \subseteq Z(M)$, since $M = BE$, $[B \cap F(M), E] \subseteq [F(M), E] = 1$ and $[B \cap F(M), B] = 1$ as B is abelian. Since $Z(M)$ is cyclic, $B \cap F(M)$ is characteristic in $Z(M)$. Since $Z(M)$ is normal in G, $\{1\} \neq B \cap F(M)$ is a normal subgroup of G contained in A, a contradiction. □

§ 8.8. Horosevskii's theorem. To conclude this section, we present a striking application of Lucchini's theorem.

Corollary 8.36 (Horosevskii). *Let G be a finite non-trivial group and $\sigma \in \mathrm{Aut}(G)$. Then $|\sigma| < |G|$.*

Proof. Let $A = \langle \sigma \rangle$ act by automorphisms on G and $\Gamma = G \rtimes A$. The group operation of Γ is

$$(g, \sigma^k)(h, \sigma^l) = (g\sigma^k(h), \sigma^{k+l}).$$

Identity A with $\{1\} \times A$ and G with $G \times \{1\}$. Since $K \cap G \subseteq A \cap G = \{1\}$ and $A \cap C_\Gamma(G) = \{1\}$,

$$K \subseteq A \cap C_\Gamma(G) = \{1\}.$$

If $k \in K$ and $g \in G$, then $gkg^{-1}k^{-1} \in G \cap K = \{1\}$ (because K and G are both normal in Γ). By Lucchini's theorem, $(A : K) < (\Gamma : A)$, that is

$$|\sigma| = |A| = (A : K) < (\Gamma : A) = |G|. \qquad \square$$

§ 8.9. *Wielandt's automorphism tower theorem. We now present without proof a beautiful theorem of Wielandt. For G a finite group with trivial center, let $A_1 = G$ and $A_{k+1} = \mathrm{Aut}(A_k)$ for $k \geq 1$. Note that identifying G with $\mathrm{Inn}(G)$, one gets a sequence

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots \tag{8.3}$$

where A_i is normal in A_{i+1}.

Definition 8.37. A group G is said to be **complete** if $Z(G) = \{1\}$ and $\mathrm{Aut}(G) = \mathrm{Inn}(G)$.

Example 8.38. For example, the group $\mathbb{S}_3$ is complete:

```
gap> G := SymmetricGroup(3);;
gap> IsTrivial(Center(G));
true
gap> AutomorphismGroup(G)=InnerAutomorphismGroup(G);
true
```

In particular, the sequence (8.3) stabilizes.

Example 8.39. Let $G = \mathbb{S}_3 \times \mathbb{S}_3$. Then $|G| = 36$ and $Z(G) = \{1\}$. Moreover, $|\mathrm{Aut}(G)| = 72$ and $|\mathrm{Aut}(\mathrm{Aut}(G))| = 144$. Since the group $\mathrm{Aut}(\mathrm{Aut}(G))$ is complete, the sequence (8.3) stabilizes. Let us do this with the computer:

```
gap> G := DirectProduct(SymmetricGroup(3),SymmetricGroup(3));;
gap> A1 := G;;
gap> A2 := AutomorphismGroup(G);;
gap> A3 := AutomorphismGroup(A2);;
gap> Order(A2);
72
gap> Order(A3);
144
gap> IsTrivial(Center(A3));
true
gap> AutomorphismGroup(A3)=InnerAutomorphismGroup(A3);
true
```

Let G be a group and $g \in G$. Let $\gamma_g \colon G \to G$, $x \mapsto gxg^{-1}$, denote the conjugation map. Then

$$\mathrm{Inn}(G) = \{\gamma_g : g \in G\}$$

is a normal subgroup of $\mathrm{Aut}(G)$. Moreover, $G/Z(G) \simeq \mathrm{Inn}(G)$.

Exercise 8.40. Let G be a non-abelian simple group, $A = \mathrm{Aut}(G)$ and $I = \mathrm{Inn}(G)$. Prove the following statements:

1) $C_A(I) = \{\mathrm{id}\}$.
2) $f(I) = I$ for all $f \in \mathrm{Aut}(A)$.
3) Every $f \in \mathrm{Aut}(A)$ is inner.
4) $\mathrm{Aut}(G)$ is complete.

The following result is known as the **Wielandt automorphism tower theorem**.

THEOREM 8.41 (Wielandt). *Let G be a finite group with trivial center. Up to isomorphism, there are finitely many groups among the terms of the sequence* (8.3).

PROOF. See [**22**, Theorem 9.10]. □

Lecture 9. 29/04/2024

§ 9.1. The transfer map. If H is a subgroup of G, recall that a **transversal** of H in G is a complete set of coset representatives of G/H.

LEMMA 9.1. *Let G be a group and H be a subgroup of G of finite index. Let R and S be transversals of H in G and let $\alpha\colon H \to H/[H,H]$ be the canonical map. Then*

$$d(R,S) = \prod \alpha(rs^{-1}),$$

where the product is taken over all pairs $(r,s) \in R \times S$ such that $Hr = Hs$, is well-defined and satisfies the following properties:

1) $d(R,S)^{-1} = d(S,R)$.
2) $d(R,S)d(S,T) = d(R,T)$ *for all transversal T of H in G.*
3) $d(Rg,Sg) = d(R,S)$ *for all $g \in G$.*
4) $d(Rg,R) = d(Sg,S)$ *for all $g \in G$.*

PROOF. The product that defines $d(R,S)$ is well-defined since $H/[H,H]$ is an abelian group. The first three claim are trivial. Let us prove 4). By 2),

$$d(Rg,Sg)d(Sg,S)d(S,R) = d(Rg,S)d(S,R) = d(Rg,R).$$

Since $H/[H,H]$ is abelian, 1) and 3) imply that

$$d(Rg,Sg)d(Sg,S)d(S,R) = d(R,S)d(S,R)d(Sg,S) = d(Sg,S). \qquad \square$$

THEOREM 9.2. *Let G be a group and H be a finite-index subgroup of G. The map*

$$\nu\colon G \to H/[H,H], \quad g \mapsto d(Rg,R),$$

does not depend on the transversal R of H in G and is a group homomorphism.

PROOF. The previous lemma implies that the map does not depend on the transversal used. Moreover, ν is a group homomorphism, as

$$\nu(gh) = d(R(gh),R) = d(R(gh),Rh)d(Rh,R) = d(Rg,R)d(Rh,R) = \nu(g)\nu(h). \qquad \square$$

The theorem justifies the following definition:

DEFINITION 9.3. Let G be a group and H be a finite-index subgroup of G. The **transfer map** of G in H is the group homomorphism

$$\nu\colon G \to H/[H,H], \quad g \mapsto d(Rg,R),$$

of Theorem 9.2, where R is some transversal of H in G.

We need methods for computing the transfer map. If H is a subgroup of G and $(G:H) = n$, let $T = \{x_1,\dots,x_n\}$ be a transversal of H. For $g \in G$ let

$$\nu(g) = \prod \alpha(xy^{-1}),$$

where the product is taken over all pairs $(x,y) \in (Tg) \times T$ such that $Hx = Hy$ and $\alpha\colon H \to H/[H,H]$ is the canonical map. If we write $x = x_i g$ for some $i \in \{1,\dots,n\}$, then $Hx_i g = Hx_{\sigma(i)}$ for some permutation $\sigma \in \mathbb{S}_n$. Thus

$$\nu(g) = \prod_{i=1}^{n} \alpha(x_i g x_{\sigma(i)}^{-1}).$$

The cycle structure of σ turns out to be important. For example, if $\sigma = (12)(345)$ and $n = 5$, then a direct calculation shows that

$$\prod_{i=1}^{5} \alpha\left(x_i g x_{\sigma(i)}^{-1}\right) = \alpha(x_1 g^2 x_1^{-1})\alpha(x_3 g^3 x_3^{-1}).$$

This is precisely the content of the following lemma.

LEMMA 9.4. *Let G be a group and H be a subgroup of index n. Let $T = \{t_1, \ldots, t_n\}$ be a transversal of H in G. For each $g \in G$ there exist $m \in \mathbb{Z}_{>0}$ and elements $s_1, \ldots, s_m \in T$ and positive integers $n_1, \ldots, n_m$ such that $s_i^{-1} g^{n_i} s_i \in H$, $n_1 + \cdots + n_m = n$ and*

$$\nu(g) = \prod_{i=1}^{m} \alpha(s_i^{-1} g^{n_i} s_i).$$

PROOF. For each i there exist $h_1, \ldots, h_n \in H$ and $\sigma \in \mathbb{S}_n$ such that $g t_i = t_{\sigma(i)} h_i$. Write σ as a product of disjoint cycles, say

$$\sigma = \alpha_1 \cdots \alpha_m.$$

Let $i \in \{1, \ldots, n\}$ and write $\alpha_i = (j_1 \cdots j_{n_i})$. Since

$$g t_{j_k} = t_{\sigma(j_k)} h_{j_k} = \begin{cases} t_{j_1} h_{j_k} & \text{si } k = n_i, \\ t_{j_{k+1}} h_{j_k} & \text{otherwise,} \end{cases}$$

then

$$\begin{aligned} t_{j_1}^{-1} g^{n_i} t_{j_1} &= t_{j_1}^{-1} g^{n_i - 1} g t_{j_1} \\ &= t_{j_1}^{-1} g^{n_i - 1} t_{j_2} h_{j_1} \\ &= t_{j_1}^{-1} g^{n_i - 2} g t_{j_2} h_{j_1} \\ &= t_{j_1}^{-1} g^{n_i - 2} t_{j_3} h_{j_2} h_{j_1} \\ &\vdots \\ &= t_{j_1}^{-1} g t_{j_{n_i}} h_{n_{i-1}} \cdots h_{j_2} h_{j_1} \\ &= t_{j_1}^{-1} t_{j_1} h_{j_{n_i}} \cdots h_{j_2} h_{j_1} \in H. \end{aligned}$$

Thus $s_i = t_{j_1} \in T$. It only remains to note that $\nu(g) = h_1 \cdots h_n$. □

Gauss's lemma in number theory gives conditions for an integer to be a quadratic residue. The lemma appears in some proof of the quadratic reciprocity. Gauss's Lemma is basically a computation of the transfer homomorphism.

EXERCISE 9.5 (Gauss' lemma). Let p be a prime number. Let $G = \mathbb{F}_p^\times$ and $H = \{-1, 1\}$.

1) Prove that the transfer homomorphism

$$\nu\colon G \to H, \quad \nu(x) = x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a square,} \\ -1 & \text{otherwise.} \end{cases}.$$

2) For a transversal $T = \{1, 2, \ldots, \frac{p-1}{2}\}$ and elements $x \in G$ and $t \in T$, let

$$\varepsilon(x,t) = \begin{cases} 1 & \text{si } xt \in T, \\ -1 & \text{si } xt \notin T. \end{cases}$$

Prove that

$$\left(\frac{x}{p}\right) = \prod_{t \in T} \varepsilon(x,t).$$

§ 9.2. Other applications of the transfer homomorphism.

LEMMA 9.6. *Let G be a group, H be a finite-index subgroup and $n = (G : H)$. Let $S = \{s_1, \ldots, s_n\}$ and $T = \{t_1, \ldots, t_n\}$ be transversals of H in G. For each $g \in G$, there exist unique $h_1, \ldots, h_n \in H$ and $\sigma \in \mathbb{S}_n$ such that*

$$gt_i = s_{\sigma(i)} h_i, \quad i \in \{1, \ldots, n\}.$$

PROOF. If $i \in \{1, \ldots, n\}$, there exists a unique $j \in \{1, \ldots, n\}$ such that $gt_i \in s_j H$. Thus $gt_i = s_j h_i$ for a unique $h_i \in H$. Thus we have constructed a $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$, $\sigma(i) = j$. We need to show that $\sigma \in \mathbb{S}_n$. It is enough to prove that σ is injective. If $\sigma(i) = \sigma(k) = j$, since $gt_i = s_j h_i$ and $gt_k = s_j h_k$, we obtain that $t_i^{-1} t_k = h_i^{-1} h_k \in H$. Hence $i = k$, since $t_i H = t_k H$. □

THEOREM 9.7. *Let G be a finite group and p be a prime number dividing $|[G,G] \cap Z(G)|$. If $P \in \mathrm{Syl}_p(G)$, then P is non-abelian.*

PROOF. Assume that P is abelian. Let $T = \{t_1, \ldots, t_n\}$ be a transversal of P in G. Since $[G,G] \cap Z(G)$ is a normal subgroup of G, we may assume that $P \cap [G,G] \cap Z(G) \neq \{1\}$. Let $z \in P \cap [G,G] \cap Z(G) \setminus \{1\}$.

Let $\nu\colon G \to P$ be the transfer homomorphism. We compute $\nu(z)$ with Lemma 9.6. For $i \in \{1, \ldots, n\}$, let $x_1, \ldots, x_n \in P$ and $\sigma \in \mathbb{S}_n$ be such that $zt_i = t_{\sigma(i)} x_i$. Since $z \in Z(G)$, $t_i = t_{\sigma(i)} x_i z^{-1}$. By the uniqueness of Lemma 9.6, $\sigma = \mathrm{id}$ and $x_i = z$ for all i. Therefore

$$\nu(z) = z^{|T|} = z^{(G:P)}.$$

Since P is abelian, $[G,G] \subseteq \ker \nu$. Thus $\nu(z) = 1$, a contradiction, since $1 \neq z \in P$ y $z^{(G:P)} = 1$ implies that z has order not divisible by p. □

Another application:

PROPOSITION 9.8. *If G is a group such that $Z(G)$ has finite index n, then $(gh)^n = g^n h^n$ for all $g, h \in G$.*

PROOF. Note that we may assume that $\alpha = \mathrm{id}$, as $Z(G)$ is abelian. Let $g \in G$. By Lemma 9.4 there are positive integers $n_1, \ldots, n_k$ such that $n_1 + \cdots + n_k = n$ and elements $t_1, \ldots, t_k$ of a transversal of $Z(G)$ in G such that

$$\nu(g) = \prod_{i=1}^{k} t_i g^{n_1} t_i^{-1}.$$

Since $g^{n_i} \in Z(G)$ for all $i \in \{1,\dots,k\}$ (as $t_i g^{n_i} t_i^{-1} \in Z(G)$), it follows that

$$\nu(g) = g^{n_1+\cdots+n_k} = g^n.$$

Now Theorem 9.2 implies the claim. □

The same idea implies the following property:

EXERCISE 9.9. If G is a group and K is a central subgroup of finite index n, then $(gh)^n = g^n h^n$ for all $g,h \in G$.

PROPOSITION 9.10. *Let G be a finite group and H a central subgroup of index n, where n is coprime with $|H|$. Then $G \simeq N \rtimes H$.*

PROOF. Since H is abelian, $H = H/[H,H]$. Let $\nu\colon G \to H$ be the transfer map and $h \in H$. By Lemma 9.4,

$$\nu(h) = \prod_{i=1}^{m} s_i^{-1} h^{n_i} s_i,$$

where each $s_i^{-1} h^{n_i} s_i \in H$. Since $h^{n_i} \in H \subseteq Z(G)$ for all i, it follows that $s_i^{-1} h^{n_i} s_i = h^{n_i}$ for all i. Thus

$$\nu(h) = \prod_{i=1}^{m} s_i^{-1} h^{n_i} s_i = \prod_{i=1}^{m} h^{n_i} = h^{\sum_{i=1}^m n_i} = h^n.$$

The composition $f\colon H \hookrightarrow G \xrightarrow{\nu} H$ is a group homomorphism. We claim that it is an isomorphism. It is injective: If $h^n = 1$, then $|h|$ divides both $|H|$ and n. Since n and $|H|$ are coprime, $h = 1$. It is surjectice: Since n and $|H|$ are coprime, there exists $m \in \mathbb{Z}$ such that $nm \equiv 1 \bmod |H|$. If $h \in H$, then $h^m \in H$ and $\nu(h^m) = h^{nm} = h$.

Let $N = \ker f$. We claim that $G = N \rtimes H$. By definition, N is normal in G and $N \cap H = \{1\}$. To show that $G = NH$ note that $|NH| = |N||H|$ and $G/N \simeq H$. □

EXERCISE 9.11. Let H be a central subgroup of a finite group G. If $|H|$ and $|G/H|$ are coprime, then $G \simeq H \times G/H$.

We now present a nice application to infinite groups taken from Serre's book [**29**, 7.12].

THEOREM 9.12. *Let G be a torsion-free group that contains a finite-index subgroup isomorphic to $\mathbb{Z}$. Then $G \simeq \mathbb{Z}$.*

PROOF. We may assume that G contains a finite-index normal subgroup isomorphic to $\mathbb{Z}$. Indeed, if H is a finite-index subgroup of G such that $H \simeq \mathbb{Z}$, then $K = \cap_{x\in G} xHx^{-1}$ is a non-trivial normal subgroup of G (because $K = \mathrm{Core}_G(H)$ and G has no torsion) and hence $K \simeq \mathbb{Z}$ (because $K \subseteq H$) and $(G:K) = (G:H)(H:K)$ is finite. The action of G on K by conjugation induces a group homomorphism $\varepsilon\colon G \to \mathrm{Aut}(K)$. Since $\mathrm{Aut}(K) \simeq \mathrm{Aut}(\mathbb{Z}) = \{-1,1\}$, there are two cases to consider.

Assume first that $\varepsilon = \mathrm{id}$. Since $K \subseteq Z(G)$, let $\nu\colon G \to K$ be the transfer homomorphism. By Proposition 9.8 (more precisely, by Exercise 9.9), $\nu(g) = g^n$, where $n = (G:K)$. Since G has no torsion, ν is injective. Thus $G \simeq \mathbb{Z}$ because it is isomorphic to a subgroup of K.

Assume now that $\varepsilon \neq \mathrm{id}$. Let $N = \ker\varepsilon \neq G$. Since $K \simeq \mathbb{Z}$ is abelian, $K \subseteq N$. The result proved in the previous paragraph applied to $\varepsilon|_N = 1$ implies that $N \simeq \mathbb{Z}$, as N contains a finite-index subgroup isomorphic to $\mathbb{Z}$. Let $g \in G \setminus N$. Since N is normal in G, G acts by conjugation on

N and hence there exists a group homomorphism $c_g \in \mathrm{Aut}(N) \simeq \{-1,1\}$. Since $K \subseteq N$ y g acts non-trivially on K,

$$c_g(n) = gng^{-1} = n^{-1}$$

for all $n \in N$. Since $g^2 \in N$,

$$g^2 = gg^2g^{-1} = g^{-2}.$$

Therefore $g^4 = 1$, a contradiction since $g \neq 1$ and G has no torsion. □

§ 9.3. Dietzman's theorem.

THEOREM 9.13 (Dietzmann). *Let G be a group and $X \subseteq G$ be a finite subset of G closed by conjugation. If there exists n such that $x^n = 1$ for all $x \in X$, then $\langle X \rangle$ is a finite subgroup of G.*

PROOF. Let $S = \langle X \rangle$. Since $x^{-1} = x^{n-1}$, every element of S can be written as a finite product of elements of X. Fix $x \in X$. We claim that if $x \in X$ appears $k \geq 1$ times in the word s, then we can write s as a product of m elements of X, where the first k elements are equal to x. Suppose that

$$s = x_1x_2 \cdots x_{t-1}xx_{t+1} \cdots x_m,$$

where $x_j \neq x$ for all $j \in \{1,\ldots,t-1\}$. Then

$$s = x(x^{-1}x_1x)(x^{-1}x_2x) \cdots (x^{-1}x_{t-1}x)x_{t+1} \cdots x_m$$

is a product of m elements of X since X is closed under conjugation and the first element is x. The same argument implies that s can be written as

$$s = x^k y_{k+1} \cdots y_m,$$

where each y_j belongs to $X \setminus \{x\}$.

Let $s \in S$ and write s as a product of m elements of X, where m is minimal. We need to show that $m \leq (n-1)|X|$. If $m > (n-1)|X|$, then at least one $x \in X$ appears exactly n times in the representation of s. Without loss of generality, we write

$$s = x^n x_{n+1} \cdots x_m = x_{n+1} \cdots x_m,$$

a contradiction to the minimality of m. □

§ 9.4. Schur's commutator theorem.

THEOREM 9.14 (Schur). *Let G be a group. If $Z(G)$ has finite index in G, then $[G,G]$ is finite.*

PROOF. Let $n = (G : Z(G))$ and X be the set of commutators of G. We claim that X is finite, in fact $|X| \leq n^2$. A routine calculation shows that the map

$$\varphi \colon X \to G/Z(G) \times G/Z(G), \quad [x,y] \mapsto (xZ(G), yZ(G)),$$

is well-defined. It is, moreover, injective: if $(xZ(G), yZ(G)) = (uZ(G), vZ(G))$, then $u^{-1}x \in Z(G)$, $v^{-1}y \in Z(G)$. Thus

$$[u,v] = uvu^{-1}v^{-1} = uv(u^{-1}x)x^{-1}v^{-1} = xvx^{-1}(v^{-1}y)y^{-1} = xyx^{-1}y^{-1} = [x,y].$$

Moreover, X is closed under conjugation, as

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

for all $g,x,y \in G$. Since $G \to Z(G)$, $g \mapsto g^n$ is a group homomorphism, Proposition 9.8 implies that $[x,y]^n = [x^n,y^n] = 1$ for all $[x,y] \in X$. The theorem follows from applying Dietzmann's theorem. □

EXERCISE 9.15. Let G be the group with generators a,b,c and relations $ab = ca$, $ac = ba$ and $bc = ab$. Prove the following statements:

1) G is infinite and non-abelian.
2) $Z(G)$ has finite index in G and every conjugacy class of G is finite.
3) $[G,G]$ is finite.
4) The subgroup $N = \langle a^3 \rangle$ of G generated by a^3 is central and G/N is finite.

We conclude the section with some results similar to that of Schur.

THEOREM 9.16 (Niroomand). *If the set of commutators of a group G is finite, then $[G,G]$ is finite.*

PROOF. Let $C = \{[x_1,y_1],\dots,[x_k,y_k]\}$ be the (finite) set of commutators of G and

$$H = \langle x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_k \rangle.$$

Since C is a set of commutators of H, it follows that $[G,G] = \langle C \rangle \subseteq [H,H]$. To simplify the notation we write $H = \langle h_1, \dots, h_{2k} \rangle$. Since $h \in Z(H)$ if and only if $h \in C_H(h_i)$ for all $i \in \{1,\dots,2k\}$, we conclude that $Z(H) = C_H(h_1) \cap \cdots \cap C_H(h_{2k})$. Moreover, if $h \in H$, then $hh_ih^{-1} = ch_i$ for some $c \in C$. Thus the conjugacy class of each h_i contains at most as many elements as C. This implies that

$$|H/Z(H)| = |H/\cap_{i=1}^{2k} C_H(h_i)| \leq \prod_{i=1}^{2k} (H : C_H(h_i)) \leq |C|^{2k}.$$

Since $H/Z(H)$ is finite, $[H,H]$ is finite. Hence $[G,G] = \langle C \rangle \subseteq [H,H]$ is a finite group. □

THEOREM 9.17 (Hilton–Niroomand). *Let G be a finitely generated group. If $[G,G]$ is finite and $G/Z(G)$ is generated by n elements, then*

$$|G/Z(G)| \leq |[G,G]|^n.$$

PROOF. Assume that $G/Z(G) = \langle x_1Z(G), \dots, x_nZ(G) \rangle$. Let

$$f\colon G/Z(G) \to [G,G] \times \cdots \times [G,G], \quad y \mapsto ([x_1,y],\dots,[x_n,y]).$$

Note that f is well-defined: If $y \in G$ y $z \in Z(G)$, then $[x_i,y] = [x_i,yz]$ for all i. Then $f(yz) = f(y)$.

The map f is injective. Assume that $f(xZ(G)) = f(yZ(G))$. Then $[x_i,x] = [x_i,y]$ for all $i \in \{1,\dots,n\}$. For each i we compute

$$\begin{aligned}[x^{-1}y,x_i] &= x^{-1}[y,x_i]x[x^{-1},x_i] \\ &= x^{-1}[y,x_i][x_i,x]x = x^{-1}[x_i,y]^{-1}[x_i,x]x = x^{-1}[x_i,y]^{-1}[x_i,y]x = 1.\end{aligned}$$

This implies that $x^{-1}y \in Z(G)$. Indeed, since every $g \in G$ can be written as $g = x_kz$ for some $k \in \{1,\dots,n\}$ and some $z \in Z(G)$, it follows that

$$[x^{-1}y, g] = [x^{-1}y, x_kz] = [x^{-1}y, x_k] = 1.$$

Since f is injective, $|G/Z(G)| \leq |[G,G]|^n$. □

EXERCISE 9.18. Prove Theorem 9.17 from Theorem 9.16.

§ 9.5. *Units in group algebras and Gardam's example. Let K be a field and G be a group. A unit $u \in K[G]$ is said to be **trivial** if $u = \lambda g$ for some $\lambda \in K \setminus \{0\}$ and $g \in G$.

EXERCISE 9.19. Prove that $\mathbb{C}[C_2]$ and $\mathbb{C}[C_5]$ have non-trivial units.

The following question is usually attributed to Kaplansky.

QUESTION 9.20 (Units in groups algebras). Let K be a field and G be a torsion-free group. Is it true that all units of $K[G]$ are trivial?

Question 9.20 was negatively answered by Gardam.

DEFINITION 9.21. The **Promislow group** is the group

$$P = \langle a, b : a^{-1}b^2a = b^{-2}, b^{-1}a^2b = a^{-2} \rangle.$$

The Promislow group P is torsion-free and the subgroup $N = \langle a^2, b^2, (ab)^2 \rangle$ is normal in P, free-abelian of rank three and $P/N \simeq C_2 \times C_2$. Moreover, the map $P \to \mathbf{GL}_2(\mathbb{Q})$ given by

$$a \mapsto \begin{pmatrix} 1 & 0 & 0 & 1/2 \\ 0 & -1 & 0 & 1/2 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & -1 & 1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

is a faithful representation. These facts appear in Passman's book [**27**].

THEOREM 9.22 (Gardam). *Let $\mathbb{F}_2$ be the field of two elements. Consider the elements $x = a^2$, $y = b^2$ and $z = (ab)^2$ of P and let*

$$p = (1+x)(1+y)(1+z^{-1}), \qquad q = x^{-1}y^{-1} + x + y^{-1}z + z,$$
$$r = 1 + x + y^{-1}z + xyz, \qquad s = 1 + (x + x^{-1} + y + y^{-1})z^{-1}.$$

Then $u = p + qa + rb + sab$ is a non-trivial unit in $\mathbb{F}_2[P]$.

PROOF. See [**12**]. □

EXERCISE 9.23. Let p be a prime number and $\mathbb{F}_p$ be the field of size p. Use the technique for proving Gardam's theorem to prove Murray's theorem on the existence on non-trivial units in $\mathbb{F}_p[P]$. Reference: arXiv:2106.02147.

Gardam also constructed non-trivial units in $\mathbb{C}[P]$.

§ 9.6. *The Alperin–Kuo theorem.

THEOREM 9.24 (Alperin–Kuo). *Let G be a finite group and $A = [G,G] \cap Z(G)$. Then $g^{(G:A)} = 1$ for all $g \in G$.*

One way to prove Theorem 9.24 uses non-trivial properties of the transfer map. More precisely, the proof of the Alperin–Kuo theorem combines the transitivity of the transfer (see [**22**, Theorem 10.8]) with the following theorem:

THEOREM 9.25 (Furtwrängler). *Let G be a finite group. Then the transfer homomorphism $G \to G^{(1)}/G^{(2)}$ is the trivial map.*

PROOF. See [**22**, Theorem 10.18] for a ring-theoretical proof. □

§ 9.7. *Passman's theorem. We now describe some other well-known problems in the theory of group rings.

Definition 9.26. A ring R is **reduced** if for all $r \in R$ such that $r^2 = 0$ one has $r = 0$.

Integral domains and boolean rings are reduced. The ring $\mathbb{Z}/8$ of integers modulo eight and $M_2(\mathbb{R})$ are not reduced.

Example 9.27. The ring over the abelian group $\mathbb{Z}^n$ with multiplication

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$

is reduced.

The structure of reduced rings is described by the Andrunakevic–Rjabuhin theorem. It states that a ring is reduced if and only if it is a subdirect products of domains. See [**13**, 3.20.5] for a proof.

Question 9.28 (Reduced group algebras). Let K be a field and G be a torsion-free group. Is it true that $K[G]$ is reduced?

Recall that if R is a unitary ring, one proves that the Jacobson radical $J(R)$ is the set of elements x such that $1 + \sum_{i=1}^{n} r_i x s_i$ is invertible for all n and all $r_i, s_i \in R$.

Question 9.29 (Semisimple group algebras). Let K be a field and G be a torsion-free group. It is true that $J(K[G]) = \{0\}$ if G is non-trivial?

Recall that an element e of a ring is said to be *idempotent* if $e^2 = e$. Examples of idempotents are 0 and 1 and these are known as the **trivial idempotents**.

Question 9.30 (Idempotents in group algebras). Let G be a torsion-free group and $\alpha \in K[G]$ be an idempotent. Is it true that $\alpha \in \{0, 1\}$?

Exercise 9.31. Prove that if $K[G]$ has no zero-divisors and $\alpha \in K[G]$ is an idempotent, then $\alpha \in \{0, 1\}$.

Exercise 9.32. Let K be a field of characteristic two. Prove that $K[C_4]$ contains non-trivial zero divisors and every idempotent of $K[C_4]$ is trivial. What happens if the characteristic of K is not two?

For completeness, let us restate Conjecture 6.29 as follows:

Question 9.33 (Zero divisors in group algebras). Let K be a field and G be a torsion-free group. Is it true that $K[G]$ is a domain?

Our goal is the prove the following implications:

$$9.29 \Longleftarrow 9.20 \Longrightarrow 9.28 \Longleftrightarrow 9.33$$

We first prove that an affirmative solution to Question 9.20 yields a solution to Question 9.28.

Theorem 9.34. *Let K be a field of characteristic $\neq 2$ and G be a non-trivial group. Assume that $K[G]$ has only trivial units. Then $K[G]$ is reduced.*

PROOF. Let $\alpha \in K[G]$ be such that $\alpha^2 = 0$. We claim that $\alpha = 0$. Since $\alpha^2 = 0$,

$$(1-\alpha)(1+\alpha) = 1-\alpha^2 = 1,$$

it follows that $1-\alpha$ is a unit of $K[G]$. Since units of $K[G]$ are trivial, there exist $\lambda \in K \setminus \{0\}$ and $g \in G$ such that $1-\alpha = \lambda g$. We claim that $g = 1$. If not,

$$0 = \alpha^2 = (1-\lambda g)^2 = 1 - 2\lambda g + \lambda^2 g^2,$$

a contradiction. Therefore $g = 1$ and hence $\alpha = 1-\lambda \in K$. Since K is a field, one concludes that $\alpha = 0$. □

EXERCISE 9.35. What happens in Theorem 9.34 if K is a field of characteristic two?

We now prove that an affirmative solution to Question 9.20 also yields a solution to Question 9.29.

THEOREM 9.36. *Let K be a field and G be a non-trivial group. Assume that $K[G]$ has only trivial units. If $|K| > 2$ or $|G| > 2$, then $J(K[G]) = \{0\}$.*

PROOF. Let $\alpha \in J(K[G])$. There exist $\lambda \in K \setminus \{0\}$ and $g \in G$ such that $1-\alpha = \lambda g$. We claim that $g = 1$. Assume $g \neq 1$. If $|K| \geq 3$, then there exist $\mu \in K \setminus \{0,1\}$ such that

$$1 - \alpha\mu = 1 - \mu + \lambda\mu g$$

is a non-trivial unit, a contradiction. If $|G| \geq 3$, there exists $h \in G \setminus \{1, g^{-1}\}$ such that

$$1 - \alpha h = 1 - h + \lambda g h$$

is a non-trivial unit, a contradiction. Thus $g = 1$ and hence $\alpha = 1-\lambda \in K$. Therefore $1+\alpha h$ is a trivial unit for all $h \neq 1$ and hence $\alpha = 0$. □

EXERCISE 9.37. Prove that if $G = \langle g \rangle \simeq \mathbb{Z}/2$, then $J(\mathbb{F}_2[G]) = \{0, g-1\} \neq \{0\}$.

We now want to prove that an affirmative answer to Question 9.28 yields an affirmative answer to Question 9.33. We first need some preliminaries.

PROPOSITION 9.38. *If G is a torsion-free group such that $\Delta(G) = G$, then G is abelian.*

PROOF. Let $x, y \in G = \Delta(G)$ and $S = \langle x, y \rangle$. The group $Z(S) = C_S(x) \cap C_S(y)$ has finite index, say n, in S. By Proposition 9.8, the map $S \to Z(S)$, $s \mapsto s^n$, is a group homomorphism. Thus

$$[x,y]^n = (xyx^{-1}y^{-1})^n = x^n y^n x^{-n} y^{-n} = 1$$

as $x^n \in Z(S)$. Since G is torsion-free, $[x,y] = 1$. □

LEMMA 9.39 (Neumann). *Let $H_1, \ldots, H_m$ be subgroups of G. Assume there are finitely many elements $a_{ij} \in G$, $1 \leq i \leq m$, $1 \leq j \leq n$, such that*

$$G = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} H_i a_{ij}.$$

Then some H_i has finite index in G.

PROOF. We proceed by induction on m. The case $m = 1$ is trivial. Let us assume that $m \geq 2$. If $(G : H_1) = \infty$, there exists $b \in G$ such that

$$H_1 b \cap \left(\bigcup_{j=1}^{n} H_1 a_{1j} \right) = \emptyset.$$

Since $H_1 b \subseteq \bigcup_{i=2}^{m} \bigcup_{j=1}^{n} H_i a_{ij}$, it follows that

$$H_1 a_{1k} \subseteq \bigcup_{i=2}^{m} \bigcup_{j=1}^{n} H_1 a_{ij} b^{-1} a_{1k}.$$

Hence G can be covered by finitely many cosets of $H_2, \ldots, H_m$. By the inductive hypothesis, some of these H_j has finite index in G. □

We now consider a projection operator of group algebras. If G is a group and H is a subgroup of G, let

$$\pi_H \colon K[G] \to K[H], \quad \pi_H \left(\sum_{g \in G} \lambda_g g \right) = \sum_{g \in H} \lambda_g g.$$

If R and S are rings, a (R,S)-bimodule is an abelian group M that is both a left R-module and a right S-module and the compatibility condition

$$(rm)s = r(ms)$$

holds for all $r \in R$, $s \in S$ and $m \in M$.

EXERCISE 9.40. Let G be a group and H be a subgroup of G. Prove that if $\alpha \in K[G]$, then π_H is a $(K[H], K[H])$-bimodule homomorphism with usual left and right multiplications,

$$\pi_H(\beta \alpha \gamma) = \beta \pi_H(\alpha) \gamma$$

for all $\beta, \gamma \in K[H]$.

LEMMA 9.41. *Let X be a left transversal of H in G. Every $\alpha \in K[G]$ can be written uniquely as*

$$\alpha = \sum_{x \in X} x \alpha_x,$$

where $\alpha_x = \pi_H(x^{-1}\alpha) \in K[H]$.

PROOF. Let $\alpha \in K[G]$. Since $\operatorname{supp} \alpha$ is finite, $\operatorname{supp} \alpha$ is contained in finitely many cosets of H, say $x_1 H, \ldots, x_n H$, where each x_j belongs to X. Write $\alpha = \alpha_1 + \cdots + \alpha_n$, where $\alpha_i = \sum_{g \in x_i H} \lambda_g g$. If $g \in x_i H$, then $x_i^{-1} g \in H$ and hence

$$\alpha = \sum_{i=1}^{n} x_i (x_i^{-1} \alpha_i) = \sum_{x \in X} x \alpha_x$$

with $\alpha_x \in K[H]$ for all $x \in X$. For the uniqueness, note that for each $x \in X$ the previous exercise implies that

$$\pi_H(x^{-1}\alpha) = \pi_H \left(\sum_{y \in X} x^{-1} y \alpha_y \right) = \sum_{y \in X} \pi_H(x^{-1} y) \alpha_y = \alpha_x,$$

as

$$\pi_H(x^{-1}y) = \begin{cases} 1 & \text{si } x = y, \\ 0 & \text{si } x \neq y. \end{cases}$$ □

LEMMA 9.42. *Let G be a group and H be a subgroup of G. If I is a non-zero left ideal of $K[G]$, then $\pi_H(I) \neq \{0\}$.*

PROOF. Let X be a left transversal of H in G and $\alpha \in I \setminus \{0\}$. By Lemma 9.41 we can write $\alpha = \sum_{x \in X} x\alpha_x$ with $\alpha_x = \pi_H(x^{-1}\alpha) \in K[H]$ for all $x \in X$. Since $\alpha \neq 0$, there exists $y \in X$ such that $0 \neq \alpha_y = \pi_H(y^{-1}\alpha) \in \pi_H(I)$ ($y^{-1}\alpha \in I$ since I is a left ideal). □

EXERCISE 9.43. Let G be a group, H be a subgroup of G and $\alpha \in K[H]$. The following statements hold:

1) α is invertible in $K[H]$ if and only if α is invertible in $K[G]$.
2) α is a zero divisor of $K[H]$ if and only if α is a zero divisor of $K[G]$.

LEMMA 9.44 (Passman). *Let G be a group and $\gamma_1, \gamma_2 \in K[G]$ be such that $\gamma_1 K[G] \gamma_2 = \{0\}$. Then $\pi_{\Delta(G)}(\gamma_1)\pi_{\Delta(G)}(\gamma_2) = \{0\}$.*

PROOF. It is enough to show that $\pi_{\Delta(G)}(\gamma_1)\gamma_2 = \{0\}$, as in this case

$$\{0\} = \pi_{\Delta(G)}(\pi_{\Delta(G)}(\gamma_1)\gamma_2) = \pi_{\Delta}(\gamma_1)\pi_{\Delta(G)}(\gamma_2).$$

Write $\gamma_1 = \alpha_1 + \beta_1$, where

$$\begin{aligned} \alpha_1 &= a_1u_1 + \cdots + a_ru_r, & & u_1, \ldots, u_r \in \Delta(G), \\ \beta_1 &= b_1v_1 + \cdots + b_sv_s, & & v_1, \ldots, v_s \notin \Delta(G), \\ \gamma_2 &= c_1w_1 + \cdots + c_tw_t, & & w_1, \ldots, w_t \in G. \end{aligned}$$

The subgroup $C = \bigcap_{i=1}^{r} C_G(u_i)$ has finite index in G. Assume that

$$0 \neq \pi_{\Delta}(\gamma_1)\gamma_2 = \alpha_1\gamma_2.$$

Let $g \in \operatorname{supp}(\alpha_1\gamma_2)$. If v_i is a conjugate in G of some gw_j^{-1}, let $g_{ij} \in G$ be such that $g_{ij}^{-1}v_ig_{ij} = gw_j^{-1}$. If v_i and gw_j^{-1} are not conjugate, we take $g_{ij} = 1$.

For every $x \in C$ it follows that $\alpha_1\gamma_2 = (x^{-1}\alpha_1 x)\gamma_2$. Since

$$x^{-1}\gamma_1 x\gamma_2 \in x^{-1}\gamma_1 K[G]\gamma_2 = 0,$$

it follows that

$$\begin{aligned} (a_1u_1 + \cdots + a_ru_r)\gamma_2 = \alpha_1\gamma_2 = x^{-1}\alpha_1 x\gamma_2 &= -x^{-1}\beta_1 x\gamma_2 \\ &= -x^{-1}(b_1v_1 + \cdots + b_sv_r)x(c_1w_1 + \cdots + c_tw_t). \end{aligned}$$

Now $g \in \operatorname{supp}(\alpha_1\gamma_2)$ implies that there exist i, j such that $g = x^{-1}v_ixw_j$. Thus v_i and gw_j^{-1} are conjugate and hence $x^{-1}v_ix = gw_j^{-1} = g_{ij}^{-1}v_ig_{ij}$, that is $x \in C_G(v_i)g_{ij}$. This proves that

$$C \subseteq \bigcup_{i,j} C_G(v_i)g_{ij}.$$

Since C has finite index in G, it follows that G can be covered by finitely many cosets of the $C_G(v_i)$. Every $v_i \notin \Delta(G)$, so each $C_G(v_i)$ has infinite index in G, a contradiction to Neumann's lemma. □

EXERCISE 9.45. Let K be a field and G be a torsion-free abelian group. Prove that $K[G]$ has no non-zero divisors.

THEOREM 9.46 (Passman). *Let K be a field and G be a torsion-free group. If $K[G]$ is reduced, then $K[G]$ is a domain.*

PROOF. Assume that $K[G]$ is not a domain. Let $\gamma_1, \gamma_2 \in K[G] \setminus \{0\}$ be such that $\gamma_2\gamma_1 = 0$. If $\alpha \in K[G]$, then

$$(\gamma_1\alpha\gamma_2)^2 = \gamma_1\alpha\gamma_2\gamma_1\alpha\gamma_2 = 0$$

and thus $\gamma_1\alpha\gamma_2 = 0$, as $K[G]$ is reduced. In particular, $\gamma_1 K[G]\gamma_2 = \{0\}$. Let I be the left ideal of $K[G]$ generated by γ_2. Since $I \neq \{0\}$, it follows from Lemma 9.42 that $\pi_{\Delta(G)}(I) \neq \{0\}$. Hence $\pi_{\Delta(G)}(\beta\gamma_2) \neq \{0\}$ for some $\beta \in K[G]$. Similarly, $\pi_{\Delta(G)}(\gamma_1\alpha) \neq \{0\}$ for some $\alpha \in K[G]$. Since

$$\gamma_1\alpha K[G]\beta\gamma_2 \subseteq \gamma_1 K[G]\gamma_2 = \{0\},$$

it follows that $\pi_{\Delta(G)}(\gamma_1\alpha)\pi_{\Delta(G)}(\beta\gamma_2) = \{0\}$ by Passman's lemma. Hence $K[\Delta(G)]$ has zero divisors, a contradictions since $\Delta(G)$ is an abelian group. □

§ 9.8. *The isomorphism problem for group algebras. If R is a commutative ring (with 1) and G is a group, then one defines the group ring $R[G]$. More precisely, $R[G]$ is the set of finite linear combinations

$$\sum_{g\in G} \lambda_g g$$

where $\lambda_g \in R$ and $\lambda_g = 0$ for all but finitely many $g \in G$. One easily proves that $R[G]$ is a ring with addition

$$\left(\sum_{g\in G} \lambda_g g\right) + \left(\sum_{g\in G} \mu_g g\right) = \sum_{g\in G} (\lambda_g + \mu_g)(g)$$

and multiplication

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{h\in G} \mu_h h\right) = \sum_{g,h\in G} \lambda_g\mu_h(gh).$$

Moreover, $R[G]$ is a left R-module with

$$\lambda\left(\sum_{g\in G} \lambda_g g\right) = \sum_{g\in G} (\lambda\lambda_g)g.$$

EXERCISE 9.47. Let G be a group. Prove that if $\mathbb{Z}[G] \simeq \mathbb{Z}[H]$, then $R[G] \simeq R[H]$ for any commutative ring R.

QUESTION 9.48 (The isomorphism problem). Let G and H be groups. Does $\mathbb{Z}[G] \simeq \mathbb{Z}[H]$ imply $G \simeq H$?

Although there are several cases where the isomorphism problem has an affirmative answer (e.g. abelian groups, metabelian groups, nilpotent groups, nilpotent-by-abelian groups, simple groups, abelian-by-nilpotent groups), it is false in general. In [**18**], Hertweck found a counterexample of order $2^{21}97^{28}$.

QUESTION 9.49 (The modular isomorphism problem). Let p be a prime number. Let G and H be finite p-groups and let K be a field of characteristic p. Does $K[G] \simeq K[H]$ imply $G \simeq H$?

Question 9.49 has an affirmative answer in several cases. However, this is not true in general. This question was recently answered by García, Margolis and del Río [**11**]. They found two non-isomorphic groups G and H both of order 512 such that $K[G] \simeq K[H]$ for all field K of characteristic two.

Lecture 10. 02/05/2024

Lecture 11. 16/05/2024

§ 11.1. *Burnside normal complement theorem. We first need a way of computing the transfer map.

LEMMA 11.1. *Let G be a group and let H be a subgroup of index n. Let $T = \{t_1, \dots, t_n\}$ be a transversal of H in G. For each $g \in G$, there exists $m \geq 1$ and there exist $s_1, \dots, s_m \in T$ and positive integers $n_1, \dots, n_m$ such that $s_i^{-1} g^{n_i} s_i \in H$, $n_1 + \cdots + n_m = n$, and*

$$\nu(g) = \prod_{i=1}^{m} s_i^{-1} g^{n_i} s_i.$$

PROOF. For each i, there exist $h_1, \dots, h_n \in H$ and $\sigma \in \mathbb{S}_n$ such that $g t_i = t_{\sigma(i)} h_i$. We write σ as a product of disjoint cycles

$$\sigma = \alpha_1 \cdots \alpha_m.$$

Fix $i \in \{1, \dots, n\}$ and write $\alpha_i = (j_1 \cdots j_{n_i})$. Since

$$g t_{j_k} = t_{\sigma(j_k)} h_{j_k} = \begin{cases} t_{j_1} h_{n_k} & \text{if } k = n_i, \\ t_{j_{k+1}} h_k & \text{otherwise,} \end{cases}$$

then

$$\begin{aligned} t_{j_1}^{-1} g^{n_i} t_{j_1} &= t_{j_1}^{-1} g^{n_i - 1} g t_{j_1} \\ &= t_{j_1}^{-1} g^{n_i - 1} t_{j_2} h_1 \\ &= t_{j_1}^{-1} g^{n_i - 2} g t_{j_2} h_1 \\ &= t_{j_1}^{-1} g^{n_i - 2} t_{j_3} h_2 h_1 \\ &\vdots \\ &= t_{j_1}^{-1} g t_{j_{n_i}} h_{n_{i-1}} \cdots h_2 h_1 \\ &= t_{j_1}^{-1} t_{j_1} h_{n_i} \cdots h_2 h_1 \in H. \end{aligned}$$

We then take $s_i = t_{j_1} \in T$. The result is thus demonstrated by observing that $\nu(g) = h_1 \cdots h_n$. □

LEMMA 11.2. *Let G be a finite group and let p be a prime dividing the order of G. Let $P \in \mathrm{Syl}_p(G)$. If $g, h \in C_G(P)$ are conjugate in G, then they are conjugate in $N_G(P)$.*

PROOF. Let $x \in G$ such that $g = xhx^{-1}$. Then $g \in C_G(xPx^{-1})$. Hence P and xPx^{-1} are Sylow subgroups of $C_G(g)$. By Sylow's theorem, there exists $c \in C_G(g)$ such that $P = cxP(cx)^{-1}$. Then $cx \in N_G(P)$ and

$$(cx)h(cx)^{-1} = c(xhx^{-1})c^{-1} = cgc^{-1} = g.$$ □

DEFINITION 11.3. Let G be a finite group and let p be a prime dividing the order of G. A **p-normal complement** is a normal subgroup N of G of order coprime to p such that $(G : N)$ is a power of p.

DEFINITION 11.4. A finite group is said to be **p-nilpotent** if it has a p-normal complement.

PROPOSITION 11.5. *Let G be a finite group with a p-normal complement N. Then N is a characteristic subgroup of G.*

Proof. Suppose $|G| = p^\alpha n$, where n is coprime to p, and let $\pi\colon G \to G/N$ be the canonical homomorphism. By hypothesis, N has order n. We will show that N is the unique subgroup of G of order n. If K is a subgroup of G of order n, then $\pi(K) \simeq K/K\cap N$ and hence the order of $\pi(K)$ divides n. But also the order of $\pi(K)$ divides the prime p since $\pi(K) \leq G/N$. Thus $\pi(K)$ is trivial and so $K = N$, implying that G has a unique subgroup of order n. In particular, N is a characteristic subgroup of G. □

Theorem 11.6 (Burnside's normal complement theorem). *Let G be a finite group and let p be a prime dividing $|G|$. Let $P \in \mathrm{Syl}_p(G)$ be such that $P \subseteq Z(N_G(P))$. Then G is p-nilpotent.*

Proof. The group P is abelian. Let $\nu\colon G \to P$ be the transfer homomorphism and $g \in P$. By Lemma 11.1, there exist $s_1,\dots,s_m \in G$ and there exist $n_1,\dots,n_m$ such that $n_1+\cdots+n_m = n$, $s_i^{-1}g^{n_i}s_i \in P$, and

$$\nu(g) = \prod_{i=1}^{m} s_i^{-1}g^{n_i}s_i.$$

Since P is abelian, $P \subseteq C_G(P)$. By Lemma 11.2, there exist elements $c_i \in N_G(P)$ such that

$$s_i^{-1}g^{n_i}s_i = c_i^{-1}g^{n_i}c_i.$$

Then $s_i^{-1}g^{n_i}s_i = g_i^{n_i}$, since $P \subseteq Z(N_G(P))$. Thus $\nu(g) = g^n$, where $n = (G:P)$. Since n and $|P|$ are coprime, there exist $r,s \in \mathbb{Z}$ such that $rn + s|P| = 1$. This implies that the restriction $\nu|_P$ is surjective since

$$g = (g^r)^n = \nu(g^r).$$

By the isomorphism theorem,

$$P/\ker\nu \cap P \simeq \nu(P) = P.$$

Thus $\ker\nu \cap P = \{1\}$. Moreover, $\nu(G) = \nu(P)$, since $P \supseteq \nu(G) \supseteq \nu(P) = P$.

We will show that $\ker\nu$ is a p-normal complement in G. Clearly, $\ker\nu$ is normal in G. Since $(G:\ker\nu) = |\nu(G)| = |P|$ and P is a Sylow p-subgroup, we conclude that $\ker\nu$ has order coprime to p. □

Exercise 11.7. Let G be a group and H a subgroup of G. Prove that $C_G(H)$ is a normal subgroup of $N_G(H)$ and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Exercise 11.8. Let G be a finite group and let p be the smallest prime dividing $|G|$. If some $P \in \mathrm{Syl}_p(G)$ is cyclic, then G is p-nilpotent.

Exercise 11.9. Let G be a finite group such that all its Sylow subgroups are cyclic. Then G is solvable.

Let us prove something stronger:

Proposition 11.10. *Let G be a finite group such that all its Sylow subgroups are cyclic. Then G is super-solvable.*

Proof. Suppose G is nontrivial and Let us induct on $|G|$. If p is the smallest prime dividing $|G|$, by Corollary 11.8 the group G has a normal p-complement N. By the inductive hypothesis, N is solvable. Since G/N is a p-group, it is solvable. Hence G is solvable. □

EXERCISE 11.11. Let G be a finite group whose order is square-free. Prove that G is solvable.

COROLLARY 11.12. *Let G be a non-abelian finite simple group and let p be the smallest prime dividing $|G|$. Then either p^3 divides $|G|$ or 12 divides $|G|$.*

PROOF. Let $P \in \mathrm{Syl}_p(G)$. By Corollary 11.8, P is not cyclic, so $|P| \geq p^2$. If p^3 does not divide $|G|$, then $P \simeq C_p \times C_p$ is a $\mathbb{F}_p$-vector space of dimension two. Since $|N_G(P)/C_G(P)|$ divides the order of G, the prime divisors of $|N_G(P)/C_G(P)|$ are at least p. Moreover, as $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$ by Exercise 11.7, and $\mathrm{Aut}(P) \simeq \mathbf{GL}_2(p)$ has order

$$(p^2-1)(p^2-p) = p(p+1)(p-1)^2,$$

it follows that $|N_G(P)/C_G(P)|$ divides $p(p+1)(p-1)^2$. Since P is abelian, $P \subseteq C_G(P)$. Thus $|N_G(P)/C_G(P)|$ is coprime to p, so $|N_G(P)/C_G(P)|$ divides $(p+1)(p-1)^2$. Since p is the smallest prime dividing $|G|$, $p-1$ and $|N_G(P)/C_G(P)|$ are coprime, implying that $|N_G(P)/C_G(P)|$ divides $p+1$. Furthermore, by Theorem 11.6, $|N_G(P)/C_G(P)| \neq 1$. This implies that $p = 2$, because if p is odd, the smallest prime dividing $|N_G(P)/C_G(P)|$ is at least $p+2$. Thus, $p = 2$, and consequently $|N_G(P)/C_G(P)| = 3$. Hence $|G|$ is divisible by $12 = 2^2 3$. □

THEOREM 11.13. *Let G be a finite group and let P be an abelian Sylow subgroup. Then $[G,G] \cap P \cap Z(N_G(P)) = \{1\}$.*

PROOF. Let $x \in [G,G] \cap P \cap Z(N_G(P))$ and let $\nu \colon G \to P$ be the transfer homomorphism. By Lemma 11.1, there exist $s_1, \ldots, s_m \in G$ and $n_1, \ldots, n_m$ such that $n_1 + \cdots + n_m = (G:P)$, $s_i^{-1} g^{n_i} s_i \in P$, and

$$\nu(x) = \prod_{i=1}^{m} s_i^{-1} x^{n_i} s_i.$$

Since P is abelian, $P \subseteq C_G(P)$. Then x^{n_i} and $s_i^{-1} x^{n_i} s_i$ are conjugate in $N_G(P)$ by Lemma 11.2. Since x^{n_i} is central in $N_G(P)$ and $[G,G] \subseteq \ker \nu$, it follows that $x = 1$ since $1 = \nu(x) = x^{(G:P)}$ and $x \in P$. □

COROLLARY 11.14. *Let G be a non-abelian finite group and let $P \in \mathrm{Syl}_2(G)$ such that*

$$P \simeq C_{a_1} \times \cdots \times C_{a_k}$$

with $a_1 > a_2 \geq a_3 \geq \cdots \geq a_k \geq 2$. Then G is not simple.

PROOF. Let $S = \{x^{n/2} : x \in P\}$. It's easy to see that S is a subgroup of P and S is characteristic in P, i.e., $f(S) \subseteq S$ for every $f \in \mathrm{Aut}(P)$. Since $S \simeq C_2$, we can write $S = \{1, s\}$. Then $s \in Z(N_G(P))$ because $gsg^{-1} \in S$ for every $g \in N_G(P)$. By Theorem 11.13, $s \notin [G,G]$, so $[G,G] \neq G$. If G were simple, then G would be abelian since $[G,G] = 1$. □

Finite groups whose Sylow subgroups are cyclic are solvable.

DEFINITION 11.15. A **Z-group** is a finite group G such that all its Sylow subgroups are cyclic.

DEFINITION 11.16. A group G is called *meta-cyclic* if G has a normal cyclic subgroup N such that G/N is cyclic.

EXERCISE 11.17. If G is a solvable group, then $C_G(F(G)) = F(G)$.

THEOREM 11.18. *Every Z-group is meta-cyclic.*

PROOF. Let G be a Z-group. By Proposition 11.10, G is solvable and hence the Fitting subgroup $F(G)$ satisfies $C_G(F(G)) \subseteq F(G)$.

Let us show that $F(G)$ is cyclic. Since $F(G)$ is nilpotent, $F(G)$ is the direct product of its Sylow subgroups. Since every Sylow subgroup of $F(G)$ is a p-subgroup of G, every Sylow subgroup of $F(G)$ is cyclic (as it is contained in some Sylow subgroup of G).

Since $F(G)$ is cyclic, $F(G)$ is abelian and hence $F(G) \subseteq C_G(F(G))$. If G acts on $F(G)$ by conjugation, then there is a homomorphism $\gamma\colon G \to \mathrm{Aut}(F(G))$ such that $\ker\gamma = C_G(F(G)) = F(G)$ (since $\gamma_g(x) = gxg^{-1}$). In particular, $G/F(G)$ is abelian as it is isomorphic to a subgroup of the abelian group $\mathrm{Aut}(F(G))$. Moreover, since the Sylow subgroups of $G/F(G)$ are cyclic (as they are quotients of Sylow subgroups of G), $G/F(G)$ is cyclic. □

Lecture 12. 24/05/2024

§ 12.1. *The Deaconescu–Walls theorem. Let A be a group acting on automorphisms on a finite group G. Then $C_G(A) = \{g \in G : a \cdot g = g \ \forall a \in A\}$ acts by left multiplication on the set of A-orbits by

$$c(A \cdot g) = \{c(a \cdot g) : a \in A\} = \{(a \cdot c)(a \cdot g) : a \in A\} = \{a \cdot (cg) : a \in A\} = A \cdot (cg)$$

for all $g \in G$ and $c \in C_G(A)$.

Theorem 12.1 (Deaconescu–Walls). *Let A be a group acting by automorphisms on a finite group G. Let $C = C_G(A)$ and $N = C \cap [A,G]$, where $[A,G]$ is the subgroup of G generated by $[a,g] = (a \cdot g)g^{-1}$, $a \in A$, $g \in G$. Then $(C : N)$ divides the number of A-orbits of G.*

Proof. The group C acts by left multiplication on the set Ω of A-orbits of G. Let $X = A \cdot g \in \Omega$ and C_X be the stabilizer of C in X. If $c \in C_X$, then $cX = X$. In particular, if $c \in C_X$, then $cg = a \cdot g$ for some $a \in A$, that is $c = (a \cdot g)g^{-1} = [a,g] \in [A,G]$. Thus $C_X \subseteq N$.

To show that $(C : N)$ divides $|\Omega|$, it is enough to show that $(C : N)$ divides the size of each C-orbit. If $X \in \Omega$, then $C \cdot X$ has size

$$(C : C_X) = (C : N)(N : C_X).$$

Hence $(C : N)$ divides the size of the orbit $C \cdot X$. □

Corollary 12.2. *Let G be a non-trivial finite group with $k(G)$ conjugacy classes. If the order of $Z(G)$ is coprime with $k(G)$, then $Z(G) \subseteq [G,G]$.*

Proof. The group $A = G$ acts on G by conjugation. Since $C_G(A) = Z(G)$ and $[A,G] = [G,G]$, Theorem 12.1 implies that the index $(Z(G) : Z(G) \cap [G,G])$ divides $k(G)$. Since $k(G)$ and $|Z(G)|$ are coprime, we conclude that $Z(G) = Z(G) \cap [G,G] \subseteq [G,G]$. □

Definition 12.3. Let G be a group and $f \in \mathrm{Aut}(G)$. We say that f is **central** if $f(x)x^{-1} \in Z(G)$ for all $x \in G$.

An automorphism f of a group G is central if and only if $f \in C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$.

Corollary 12.4. *Let G be a finite group with $k(G)$ conjugacy classes and $c(G)$ central automorphisms. If $\gcd(|G|, k(G)c(G)) = 1$, then $[G,G] = Z(G)$.*

Proof. By Corollary 12.2, $Z(G) \subseteq [G,G]$. Conversely, let $A = C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$. Since $|G|$ and $k(G)c(G)$ are coprime and $(C_G(A) : C_G(A) \cap [A,G])$ divides $c(G)$ by Theorem 12.1, we obtain that $C_G(A) = C_G(A) \cap [A,G]$. Since

$$a \cdot [x,y] = [(a \cdot x)x^{-1}x, (a \cdot y)y^{-1}y] = [x,y]$$

for all $a \in A$ and $x,y \in G$, $[G,G] \subseteq C_G(A)$. Moreover, $[A,G] \subseteq Z(G)$. Thus

$$[G,G] \subseteq C_G(A) = C_G(A) \cap [A,G] \subseteq [A,G] \subseteq Z(G).$$ □

Exercise 12.5. Let p be a prime number and G be a group with p conjugacy classes. Prove that either $Z(G) \subseteq [G,G]$ or $|G| = p$.

§ 12.2. *The Chermak–Delgado subgroup.

Definition 12.6. Let G be a finite group and H a subgroup of G. The **Chermak–Delgado measure** of H is the number $m_G(H) = |H||C_G(H)|$.

Example 12.7. If G is abelian and H is a subgroup of G, then $m_G(H) = |H||G|$.

Example 12.8. Let $G = \mathbb{S}_3$. The subgroups of G are

$$H_0 = 1, \quad H_1 = \langle (23) \rangle, \quad H_2 = \langle (12) \rangle, \quad H_3 = \langle (13) \rangle, \quad H_4 = \langle (123) \rangle, \quad H_5 = \mathbb{S}_3.$$

A direct calculation shows that

$$m_G(H_j) = \begin{cases} 6 & \text{if } j \in \{0,5\}, \\ 4 & \text{if } j \in \{1,2,3\}, \\ 9 & \text{if } j = 4. \end{cases}$$

Lemma 12.9. *Let G be a finite group and H be a subgroup of G. Then*

$$m_G(H) \leq m_G(C_G(H)).$$

If the equality holds, then $H = C_G(C_G(H))$.

Proof. Let $C = C_G(H)$. Since $H \subseteq C_G(C)$,

$$m_G(C) = |C||C_G(C)| \geq |C||H| = m_G(H).$$

If $m_G(H) = m_G(C_G(H))$, then $|H| = |C_G(C_G(H))|$ and hence $H = C_G(C_G(H))$, as $H \subseteq C_G(C_G(H))$. □

Lemma 12.10. *Let G be a finite group and H and ,K be subgroups of G. Let $D = H \cap K$ and $J = \langle H, K \rangle$. Then*

$$m_G(H)m_G(K) \leq m_G(D)m_G(J).$$

If the equality holds, then $J = HK$ and $C_G(D) = C_G(H)C_G(K)$.

Proof. Let $C_H = C_G(H)$, $C_K = C_G(K)$, $C_D = C_G(D)$, and $C_J = C_G(J)$. Then $C_J = C_H \cap C_K$ and $C_H \cup C_K \subseteq C_D$. Since

$$|J| \geq |HK| = \frac{|H||K|}{|D|}, \quad |C_D| \geq |C_H C_K| = \frac{|C_H||C_K|}{|C_J|},$$

we obtain that

$$m_G(D) = |D||C_D| \geq \frac{|H||K|}{|J|} \frac{|C_H||C_K|}{|C_J|} = \frac{m_G(H)m_G(K)}{m_G(J)}.$$

The second claim is clear. □

Definition 12.11. Let G be a finite group and $\mathscr{L}$ be a collection of subgroups of G. We say that $\mathscr{L}$ is a **lattice** if for every $H, K \in \mathscr{L}$ one has that $H \cap K \in \mathscr{L}$ and $\langle H, K \rangle \in \mathscr{L}$.

Since G is finite, it makes sense to consider the set $\mathscr{L}(G)$ of subgroups of G G where the Chermak–Delgado gets its largest value, say M_G.

Exercise 12.12. Let G be a finite group and H be a subgroup of G. Prove that $M_H \leq M_G$.

EXAMPLE 12.13. Let $G = \mathbb{D}_8 = \langle r,s : r^4 = s^2 = 1, srs = r^{-1}\rangle$ be the dihedral group of eight elements. In the subgroups

$$G, \quad Z(G) = \{1, r^2\}, \quad A = \{1, r, r^2, r^3\}, \quad B = \{1, s, sr^2, r^2\}, \quad C = \{1, sr, sr^3, r^2\},$$

the Chermak–Delgado measure is 16 and this is the largest possible value. Thus and $M_G = 16$ and $\mathscr{L}(G) = \{G, Z(G), A, B, C\}$.

```
gap> ChermakDelgado := function(group, subgroup)
> return Size(subgroup)\
> *Size(Centralizer(group, subgroup));
> end;
function( group, subgroup ) ... end
gap> gr := DihedralGroup(IsPermGroup, 8);;
gap> r := gr.1;;
gap> s := gr.2;;
gap> ChermakDelgado(gr, Subgroup(gr, [r]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [s*r,s*r^3]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [s,s*r^2]));
16
gap> ChermakDelgado(gr, Subgroup(gr, [r^2]));
16
gap> List(AllSubgroups(gr), x->ChermakDelgado(gr, x));
[ 8, 16, 8, 8, 8, 8, 16, 16, 16, 16 ]
```

THEOREM 12.14. *Let G be a finite group. The following statements hold:*

1) *$\mathscr{L}(G)$ is a lattice.*
2) *If $H, K \in \mathscr{L}(G)$, then $\langle H, K\rangle = HK$.*
3) *If $H \in \mathscr{L}(G)$, then $C_G(H) \in \mathscr{L}(G)$ and $C_G(C_G(H)) = H$.*

PROOF. If $H, K \in \mathscr{L}(G)$, then $m_G(H) = m_G(K) = M_G$. Let $D = H \cap K$ and $J = \langle H, K\rangle$. By Lemma 12.10,

$$M_G^2 = m_G(H)m_G(K) \leq m_G(D)m_G(J).$$

Since $m_G(D) \leq M_G$ and $m_G(J) \leq M_G$ (because M_G is the largest possible value), we conclude that $m_G(D) = m_G(J) = M_G$. Hence $\mathscr{L}(G)$ is a lattice.

Since $m_G(H)m_G(K) = m_G(D)m_G(J) = M_G^2$, Lemma 12.10 implies that $J = HK$.

By Lemma 12.9,

$$M_G = m_G(H) \leq m_G(C_G(H)).$$

Since M_G is the largest possible value, $m_G(C_G(H)) = M_G$. Thus $C_G(H) \in \mathscr{L}(G)$. By Lemma 12.9, $C_G(C_G(H)) = H$. □

Theorem 12.14 implies the existence of the **Chermak–Delgado subgroup**.

COROLLARY 12.15. *Let G be a finite group. There exists a unique subgroup M minimal suc that $m_G(M)$ is the largest possible value among all the subgroups of G. Moreover, M is characteristic, abelian and $Z(G) \subseteq M$.*

PROOF. By Theorem 12.14, $\mathscr{L}(G)$ is a lattice. Let

$$M = \bigcap_{H \in \mathscr{L}(G)} H \in \mathscr{L}(G).$$

By Theorem 12.14,

$$C_G(M) \in \mathscr{L}(G) \text{ and } M = C_G(C_G(M)) \supseteq Z(G).$$

Since $C_G(M) \in \mathscr{L}(G)$, $M \subseteq C_G(M)$. Hence M is abelian. Moreover, M is characteristic in G because $f(M) \in \mathscr{L}(G)$ for all $f \in \mathrm{Aut}(G)$. □

Example 12.16. Let $G = \mathbb{D}_8$ be the dihedral group of eight elements. The Chermak–Delgado subgroup of G is $Z(G) \simeq C_2$. See Example 12.13.

Theorem 12.17 (Chermak–Delgado). *Let G be a finite group. Then G has an abelian characteristic subgroup M such that $(G:M) \leq (G:A)^2$ for every abelian subgroup A of G.*

Proof. Let M be the Chermak–Delgado subgroup of Corollary 12.15 and A be an abelian subgroup of G. Then $A \subseteq C_G(A)$. Hence

$$m_G(M) \geq m_G(A) = |A||C_G(A)| \geq |A|^2$$

and

$$(G:A)^2 = \frac{|G|^2}{|A|^2} \geq \frac{|G|^2}{m_G(M)} = \frac{|G|}{|M|}\frac{|G|}{|C_G(M)|} = \frac{|G|}{|M|} = (G:M). \qquad \square$$

Corollary 12.18. *Let G be a non-abelian finite group and H be a subgroup of G such that*

$$|H||C_G(H)| > |G|.$$

Then G is not simple.

Proof. Let M be the Chermak–Delgado subgroup of G. Then

$$m_G(M) \geq m_G(H) > |G|. \tag{12.1}$$

This implies that $M \neq \{1\}$, since $m_G(M) = m_G(1) = |G|$. If G is simple, then $G = M$ is abelian. □

Corollary 12.19. *Let G be a non-abelian finite group and $P \in \mathrm{Syl}_p(G)$. If P is abelian and $|P|^2 > |G|$, then G is not simple.*

Proof. Let M be the Chermak–Delgado subgroup of G. Since P is abelian,

$$(G:M) \leq (G:P)^2 < |G|$$

by Theorem 12.17. Hence $M \neq \{1\}$. If G is simple, then $G = M$ is abelian. □

We now discuss an application of the Wielandt zipper theorem to the Chermak–Delgado lattice.

Lemma 12.20. *Let G be a finite group, $H \in \mathscr{L}(G)$ and S be a subgroup of G such that $HC_G(H) \subseteq S$. Then $H \in \mathscr{L}(S)$.*

Proof. Since $C_G(H) \subseteq S$, $C_G(H) = C_S(H)$. By Exercise 12.12, $M_S \leq M_G$. Thus $M_G = M_S$, since

$$M_G = m_G(H) = |H||C_G(H)| = |H||C_S(H)| = m_S(H) \leq M_S. \qquad \square$$

Theorem 12.21. *Let G be a finite group. Every $H \in \mathscr{L}(G)$ is subnormal in G.*

Proof. We proceed by induction on $|G|$. If $|G| = 1$, the result is trivial. So assume the group G is non-trivial. Let $H \in \mathscr{L}(G)$ and $K = HC_G(H)$. Since H is normal in K, by the inductive hypotehsis, it is enough to show that K is subnormal in G. If $K = G$, the claim holds. So assume that $K \neq G$.

Assume that K is not subnormal in G. By the inductive hypothesis and Wielandt's zipper theorem (Theorem 8.25), there exists a unique maximal subgroup M containing K. By Theorem 12.14,

$C_G(H) \in \mathscr{L}(G)$ and $K = HC_G(H) \in \mathscr{L}(G)$. By Lemma 12.20, $H \in \mathscr{L}(M)$. Hence $K \in \mathscr{L}(M)$. By the inductive hypothesis, K is subnormal in M. We claim that M is normal in G. Let $x \in G$. Since $m_G(xKx^{-1}) = m_G(K)$, the subgroup $xKx^{-1} \in \mathscr{L}(G)$. Hence $K(xKx^{-1}) \in \mathscr{L}(G)$.

If $K(xKx^{-1}) = G$, then, since there exist $k_1, k_2 \in K$ such that $k_1(xk_2x^{-1}) = x^{-1}$, we obtain that $x \in K$, since $x^{-1} = k_2k_1 \in K$. This implies that $xKx^{-1} \subseteq K$. Therefore $K = G$, a contradiction.

Since $K(xKx^{-1}) \neq G$, there exists a maximal subgroup N such that $K(xKx^{-1}) \subseteq N$. Since $K \subseteq N$, $N = M$ because M is the unique maximal subgroup containing K. Since $xKx^{-1} \subseteq M$, $K \subseteq x^{-1}Mx$. Hence $x^{-1}Mx = M$, because $x^{-1}Mx$ is a maximal subgroup containing K and M is the only maximal subgroup containing K. □

Corollary 12.22. *LetG be a non-abelian finite Then* $\mathscr{L}(G) = \{1, G\}$.

Proof. Let $K \in \mathscr{L}(G)$. Then K is subnormal in G by Theorem 12.21. Hence $K \in \{1, G\}$. Now the claim follows from $m_G(1) = m_G(G)$. □

Exercise 12.23. Let $n \geq 5$. Prove that $\mathscr{L}(\mathbb{S}_n) = \{1, \mathbb{S}_n\}$.

§ 12.3. Miller's double cosets theorem. Let G be a group and H and K be subgroups of G. The group $L = H \times K$ acts on G by

$$(h,k) \cdot g = hgk^{-1}, \quad h \in H, k \in K, g \in G.$$

The orbits of this action are the set of the form

$$HgK = \{hgk : h \in H, k \in K\}.$$

A set of the form HgK for some $g \in G$ is called a **double coset** modulo (H,K) with representative g. In particular, any two double cosets are either disjoint or equal, and G decomposes as a disjoint union

$$G = \bigcup_{i \in I} Hg_iK,$$

for some set I. Let

$$L_g = \{(h,k) \in H \times K : hgk^{-1} = g\} = \{(h, g^{-1}hg) \in H \times K\}.$$

Then $|L_g| = |H \cap gKg^{-1}|$, because there is a bijection $L_g \to H \cap gKg^{-1}$. By the fundamental counting principle,

$$|HgK| = (L : L_g) = \frac{|H \times K|}{|H \cap gKg^{-1}|} = \frac{|H||K|}{|H \cap gKg^{-1}|}.$$

We need a lemma.

Lemma 12.24. *Let G be a finite group, x ∈ G, and H and K be subgroups of G. Then*

$$\#\{zK : zK \subseteq HxK\} = (H : xKx^{-1} \cap H).$$

Proof. Let $L = xKx^{-1} \cap H$ and

$$\varphi \colon H/L \to \{yK : yK \subseteq H \times K\}, \quad hL \mapsto hxK.$$

The map φ is well-defined. If $hL = h_1L$, then $h^{-1}h_1 \in L$. Thus $h^{-1}h_1 = xkx^{-1}$ for some $k \in K$. This means that

$$(h_1x)^{-1}(hx) = x^{-1}h_1^{-1}hx = k \in K,$$

that is $\varphi(hL) = hxK = h_1xK = \varphi(h_1L)$.

The map φ is surjective: If zK is such that $zK \subseteq HxK$, then $z = hxk$ for some $k \in K$. In particular, $zK = hxK$. Now $\varphi(hL) = hxK = zK$.

The map φ is injective: If $hxK = h_1xK$, then $x^{-1}h_1^{-1}hx \in K$. Moreover, $h_1^{-1}h \in xKx^{-1} \cap H = L$. Thus $h_1L = hL$. □

EXERCISE 12.25. Let G be a finite group, H and K be subgroups of G, and $x \in G$. Prove that

$$\#\{Hy : Hy \subseteq HxK\} = (K : xHx^{-1} \cap K).$$

THEOREM 12.26 (Miller). *Let G be a finite group and H and K be subgroups of G of the same index. Then there exists a common complete set of representatives for the right cosets of H in G and the left cosets of K in G.*

PROOF. Let Hy be a right coset and zK be a left coset. Note that Hy and zK have a common representative if and only if $Hy \cap zK \neq \emptyset$, as

$$Hy = Hx \text{ and } zK = xK \iff xy^{-1} \in H \text{ and } z^{-1}x \in K \iff x \in Hy \cap zK.$$

The group G decomposes as a disjoint union of finitely many double cosets. Each doble coset HxK is a disjoint union of finitely many right cosets of H and a disjoint union of finitely many left cosets of K. Thus

$$HxK = \bigcup_{i=1}^{k} Hy_i = \bigcup_{j=1}^{l} z_jK,$$

where the unions are disjoint. Since $|H| = |K|$, by applying cardinality, it follows that $k = l$. To prove the theorem it is enough to show that each Hy_i intersects every z_jK.

Note that for each $i \in \{1,\dots,k\}$ there exists $j \in \{1,\dots,k\}$ such that $Hy_i \cap z_jK \neq \emptyset$. Without loss of generality, we may assume (reordering if needed) that $Hy_1 \cap z_jK \neq \emptyset$ for all $j \in \{1,\dots,m\}$, where $1 \leq m \leq k$. Then

$$Hy_1 \subseteq \bigcup_{j=1}^{m} z_jK.$$

Then

$$Hy_1K \subseteq \bigcup_{j=1}^{m} z_jK \subseteq \bigcup_{j=1}^{k} z_jK = HxK.$$

Since Hy_1K and HxK are double cosets with non-empty intersection, they are equal. Thus

$$|HxK| = |Hy_1K| \leq \sum_{j=1}^{m} |z_jK| = m|K|.$$

By Lemma 12.24,

$$k = \#\{z_jK : z_jK \subseteq HxK\} = (H : xKx^{-1} \cap H).$$

Therefore

$$k|K| = \frac{|H||K|}{|H \cap xKx^{-1}|} = |HxK| \leq m|K|$$

and hence $k = m$. □

EXERCISE 12.27 (Hall). Let G be a finite group and H be a subgroup of G with $(G : H) = n$. Then there exists $x_1,\dots,x_n \in G$ such that $\{Hx_1, Hx_2, \dots, Hx_n\} = \{x_1H, x_2H, \dots, x_nH\}$.

§ 12.4. *Landau's Theorem. In 1903, Landau demonstrated that there exists only a finite number of groups with finite conjugacy classes. The proof is entirely elementary and is based on the following lemma:

LEMMA 12.28 (Landau). *For each $k \in \mathbb{N}$, the equation*

$$\frac{1}{n_1} + \cdots + \frac{1}{n_k} = 1$$

has only finitely many solutions.

PROOF. Suppose $0 < n_1 \leq n_2 \leq \cdots \leq n_k$. Then $n_1 \leq k$. We prove by induction that

$$n_j \leq \frac{k+1-j}{1-\left(\frac{1}{n_1} + \cdots + \frac{1}{n_{j-1}}\right)}$$

for all $j \in \{2,\ldots,k\}$. Since for each $j \in \{2,\ldots,k\}$, $n_j \leq n_2$, then $1 \leq \frac{1}{n_1} + \frac{k-1}{n_2}$ and hence $n_2 \leq \frac{k-1}{1-\frac{1}{n_1}}$. If we assume that the result holds for $j \geq 2$, say $n_p \geq n_j$ for all $p \geq j$, then

$$1 \leq \sum_{i=1}^{j-1} \frac{1}{n_i} + \frac{k-j+1}{n_j},$$

which implies the inequality we wanted to prove. □

THEOREM 12.29 (Landau). *Let $k \geq 1$. There exists only a finite number of finite groups that have exactly k conjugacy classes.*

PROOF. Let G be a group with k conjugacy classes, say $C_1,\ldots,C_k$, and let $1 = g_1,\ldots,g_k$ be representatives of these classes. When we decompose G as $G = C_1 \cup \cdots \cup C_k$, we have

$$|G| = |C_1| + \cdots + |C_k| = (G : C_G(g_1)) + \cdots (G : C_G(g_k)).$$

For each $j \in \{1,\ldots,k\}$, let $n_j = |C_G(g_j)|$. Then

$$1 = \frac{1}{n_1} + \cdots + \frac{1}{n_k}.$$

As we saw in Lemma 12.28, this equation has only finitely many solutions. In particular, $n_k = |G|$ is bounded by a function of k. □

Landau's method allows tackling certain classification results. Let us see some examples.

EXAMPLE 12.30. Let G be a finite group that has two conjugacy classes. Since $G \setminus \{1\}$ is a conjugacy class, $|G|-1$ divides $|G|$, and thus $|G| = 2$.

EXAMPLE 12.31. Let G be a finite non-abelian group with three conjugacy classes. The solutions of the equation $1/n_1 + 1/n_2 + 1/n_3 = 1$ with $n_1 \leq n_2 \leq n_3$ are $(3,3,3)$, $(2,3,6)$, and $(2,4,4)$. The only possibility is $(2,3,6)$. Then $G \simeq \mathbb{S}_3$.

Now let us see a bound that can be easily obtained from Landau's method.

THEOREM 12.32 (Neumann). *If G is a finite group of order n with k conjugacy classes, then*

$$k \geq \frac{\log\log n}{\log 4}.$$

PROOF. We proceed as we did in the proof of Landau's theorem. Let $C_1, \ldots, C_k$ be the conjugacy classes, and let $1 = g_1, \ldots, g_k$ be representatives of these classes. When we decompose G as a disjoint union of conjugacy classes, we have

$$n = |G| = |C_1| + \cdots + |C_k| = (G : C_G(g_1)) + \cdots (G : C_G(g_k)).$$

For each $j \in \{1, \ldots, k\}$, let $n_j = |C_G(g_j)|$. Then

$$1 = \frac{1}{n_1} + \cdots + \frac{1}{n_k}.$$

We claim that

$$\max_{1 \le i \le k} n_i \le k^{2^{k-1}}.$$

Without loss of generality, we can assume that $n_1 \le n_2 \le \cdots \le n_k$. Then $n_1 \le k$, because otherwise,

$$\sum_{i=1}^{k} \frac{1}{n_i} < \sum_{i=1}^{k} \frac{1}{k} = 1,$$

a contradiction. Let $r \in \{1, \ldots, k-1\}$. We write

$$\sum_{i=r+1}^{k} \frac{1}{n_i} = 1 - \sum_{i=1}^{r} \frac{1}{n_i} = \frac{x}{n_1 \cdots n_r}$$

for some positive integer x. Then

$$\frac{k-r}{n_{r+1}} \ge \frac{1}{n_1 \cdots n_r}$$

and hence $n_{r+1} \le (k-r) n_1 \cdots n_r < k n_1 \cdots n_r$.

To complete the proof, we need to prove that

$$n_r \le k^{2^{r-1}} \tag{12.2}$$

for all r. We proceed by induction on r. The case $r = 1$ is trivial. Suppose then that the result is valid for all $j \le r$. By the inductive hypothesis,

$$n_{r+1} \le k n_1 \cdots n_r \le k \prod_{j=1}^{k} 2^{2^{j-1}} = k^{2^k}. \qquad \square$$

OPEN PROBLEM 12.33 (Brauer). Find good bounds for the order n of a group with a fixed number k of conjugacy classes. It is expected that the bounds will be considerably better than those obtained from Landau's method.

§ 12.5. *Burnside's cyclic numbers theorem. We now mention some problems and results related to the number of isomorphism classes of finite groups of a given order. This classification problem is obviously almost as old as group theory itself. When taking the first steps in group theory, we encounter some easy-to-prove results:

- There exists a unique finite group of prime order, and it is cyclic.
- There are two groups of order four, both abelian.
- There are two groups of order six, one of which is non-abelian.
- Groups of order p^2 are abelian.

With the Sylow theorems, we can go a bit further. It is easy to prove, for example, that there exists a unique group of order 15, and it is cyclic. The same result can be shown for other orders, such as 455 and 615.

A natural question arises. For which values of n does a unique group (which will obviously be isomorphic to C_n) of order n exist? The answer was given by Burnside.

DEFINITION 12.34. A number $n \in \mathbb{N}$ is called **cyclic** if C_n is the only group (up to isomorphism) of order n.

Some examples of cyclic numbers are: 2, 3, 15, and $615 = 3 \cdot 5 \cdot 41$.

THEOREM 12.35 (Burnside). *Let $n \in \mathbb{N}$. Then n is cyclic if and only if n and $\phi(n)$ are coprime.*

PROOF. Suppose n is cyclic. Without loss of generality, we can assume that n is square-free (because otherwise, if $n = p^a m$ with $m \in \mathbb{N}$, p prime such that $\gcd(p,m) = 1$, and $a \geq 2$, the group $C_m \times C_p^a$ has order n and is not cyclic). We then write

$$n = p_1 \cdots p_k$$

with the p_j distinct primes and $\phi(n) = (p_1 - 1) \cdots (p_k - 1)$. If $\gcd(n, \phi(n)) \neq 1$, there exist distinct primes p and q such that p divides $q - 1$. The group $G = C_m \times (C_p \rtimes C_q)$ has order $n = pqm$ and is not cyclic.

Suppose $\gcd(n, \phi(n)) = 1$ and n is not cyclic. Let G be a group of minimum order n that is not cyclic. Without loss of generality, we can assume that n is square-free: if $n = p^\alpha m$ with p prime, m coprime with p and $\alpha \geq 2$, then, as $\phi(n) = p^{\alpha-1}(p-1)\phi(m)$, p divides $\gcd(n, \phi(n))$. Then

$$n = p_1 \cdots p_k,$$

with the p_j distinct primes.

CLAIM. Every subgroup of G and every quotient of G is cyclic.

If m divides n, then $\gcd(m, \phi(m)) = 1$ since n and $\phi(n) = (p_1 - 1) \cdots (p_k - 1)$ are coprime. Therefore, every subgroup and every proper quotient is cyclic by the minimality of n.

CLAIM. $Z(G) = \{1\}$.

For each $i \in \{1, \ldots, k\}$, let $x_i \in G$ be an element of order p_i. If G were abelian, then G would be cyclic: $x_1 \cdots x_k$ would be an element of order n. Hence $Z(G) \neq G$. Now, if $1 < |Z(G)| < n$, then $G/Z(G)$ would be cyclic (since every quotient of G is), and then G would be abelian.

CLAIM. If M is a maximal subgroup of G and $x \in M \setminus \{1\}$, then $M = C_G(x)$. In particular, if M and N are distinct maximal subgroups, then $M \cap N = \{1\}$.

Since $Z(G) \neq \{1\}$, $C_G(x) \neq G$. And since M is cyclic, $M \subseteq C_G(x)$. Therefore, by maximality, $M = C_G(x)$. If M and N are two maximal subgroups and $x \in M \cap N \setminus \{1\}$, then $M = N = C_G(x)$.

CLAIM. If M is a maximal subgroup, then $M = N_G(M)$.

Let $x \in N_G(M) \setminus \{1\}$ and let $\alpha \in \mathrm{Aut}(M)$ be given by $y \mapsto xyx^{-1}$. Since M is cyclic, if $m = |M|$, then $|\mathrm{Aut}(M)|$ has order $\phi(m)$. On the other hand, since $|x|$ divides n, $|\alpha|$ divides n. Hence $|\alpha|$ divides $\gcd(n, \phi(m)) = 1$. This means that $x \in C_G(M)$, i.e., $N_G(M) \subseteq C_G(M)$. Since $M \subseteq N_G(M) \subseteq C_G(M)$, $M = N_G(M) = C_G(M)$.

Let $M_1, \ldots, M_l$ be the representatives of the conjugacy classes of maximal subgroups of G. For each $j \in \{1, \ldots, l\}$, let $m_j = |M_j|$. Since $M_j = N_G(M_j)$ for each j, the orbit of M_j has n/m_j elements.

Since for each $g \in G \setminus \{1\}$ there exists a unique maximal subgroup M such that $g \in M$, we have

$$n = 1 + \sum_{j=1}^{l} \frac{n}{m_j}(m_j - 1). \tag{12.3}$$

If $l = 1$ then $n = m_1$, a contradiction. If $l > 1$ then, since for each j we have $m_j \geq 2$, rewriting (12.3), we have

$$\frac{1}{n} + l - 1 = \sum_{j=1}^{l} \frac{1}{m_j} \leq \frac{l}{2}.$$

From this inequality, we obtain $nl \leq 2n - 2 < 2n$ and then $l < 2$, a contradiction. □

Similarly, abelian and nilpotent numbers can be defined. These numbers are classified, and an elementary proof can be found in [**26**]. There is also the notion of a solvable number. Thanks to the Feit–Thompson theorem, every odd number is a solvable number. These numbers are also classified, although the proof is much more difficult as it relies on a very deep theorem of Thompson and the famous Feit–Thompson theorem.

§ 12.6. *How many finite groups are there? In [**7**], the function $\mathrm{gnu}(n)$ is defined, which returns the number of isomorphism classes of groups of order n. For example,

$$\mathrm{gnu}(1) = \mathrm{gnu}(2) = \mathrm{gnu}(3) = \mathrm{gnu}(5) = 1 \text{ and } \mathrm{gnu}(4) = \mathrm{gnu}(6) = 2.$$

The name comes from ***gnu****mber*.

Burnside's theorem can be reformulated as follows:

$$\mathrm{gnu}(n) = 1 \iff n \text{ is cyclic} \iff \gcd(n, \phi(n)) = 1.$$

In [**7**], Conway, Dietrich, and O'Brien characterized the $n \in \mathbb{N}$ such that $\mathrm{gnu}(n) = 2$, $\mathrm{gnu}(n) = 3$, $\mathrm{gnu}(n) = 4$.

In the Encyclopedia of Integer Sequences, the sequence

$$\mathrm{gnu}(1), \mathrm{gnu}(2), \mathrm{gnu}(3), \mathrm{gnu}(4) \ldots$$

is `A000001`, see `http://oeis.org/A000001` for more information.

There exists a powerful database of small groups. It was written by Besche, Eick and O'Brien and is now a fundamental tool in group theory [**3**]. In particular, this database allows us to easily compute some values of the function gnu.

The function `NrSmallGroups` returns the number of isomorphism classes of groups of a certain order. We then define the function gnu and compute some examples:

```
gap> gnu := NrSmallGroups;;
gap> gnu(16);
14
gap> gnu(32);
51
gap> gnu(64);
267
gap> gnu(27);
5
gap> gnu(81);
15
gap> gnu(128);
2328
gap> gnu(512);
```

```
10494213
```

It is known that $\mathrm{gnu}(1024) = 49487365422$, although this value cannot be obtained directly with the computer, as there are way too many groups of order 1024. The groups of order 1024 were classified by Besche, Eick, and O'Brien, and the announcement was made in [**2**].

More than 99% of the groups of order < 2000 are of order 1024. In fact, as we saw, there are 49487365422 groups of order 1024, and the number of isomorphism classes of groups of order $n \neq 1024$ with $n < 2016$ is 423164131.

```
gap> Sum([1..1023], gnu);
423164131
```

The classification of groups is a difficult problem. A particularly difficult case is that of groups of order p^3, where p is a prime number. For example, there are exactly 2 groups of order 2^3 and 5 groups of order 3^3. For general p, the question is open. For example, there are 14 groups of order 2^4, 51 groups of order 2^5, and 267 groups of order 2^6. The sequences are found in the Encyclopedia of Integer Sequences, sequences A000679, A000880, and A000881.

```
gap> Sum([1..1023], gnu)+Sum(List([1025..2015], gnu));
423164131
```

These numbers give us approximately 99.15%.

These observations naturally suggest the following conjecture, which seems to be part of mathematical folklore:

Conjecture 12.36. Almost every finite group is a 2-group.

The numerology we did allows us to avoid having to make precise what "almost every finite group" means. Similar problems appear in Chapter 22 of the book [**4**].

Open problem 12.37. Calculate $\mathrm{gnu}(2048)$.

It is known that $\mathrm{gnu}(2048) > 1774274116992170$, which is the number of subgroups of order 2048 of a certain class.

Conjecture 12.38. x Let $n \geq 1$. The sequence

$$\mathrm{gnu}(n), \mathrm{gnu}^2(n), \mathrm{gnu}^3(n) \ldots$$

stabilizes at 1.

In Conjecture 12.38, $\mathrm{gnu}^1(n) = \mathrm{gnu}(n)$ and $\mathrm{gnu}^{k+1}(n) = \mathrm{gnu}(\mathrm{gnu}^k(n))$ for $k \geq 1$.

It is not difficult to verify that the conjecture is true for $n < 2000$.

The following conjecture appeared independently in several places. Apparently, the first more or less explicit appearance was around 1930 and was due to Miller. Independently, MacHale formulated it forty years later.

Conjecture 12.39. The function $\mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$, $n \mapsto \mathrm{gnu}(n)$, is surjective.

For more information about this conjecture, we refer to [**4**, §21.6].

Although there are many conjectures about the behavior of the function that counts the number of isomorphism classes of finite groups, there are several results. The following one is completely elementary:

Theorem 12.40. *If* $n \geq 1$, *then* $\mathrm{gnu}(n) \leq n^{n \log_2 n}$.

PROOF. If G is a group, let

$$d(G) = \min\{k : \text{there exist } g_1, \ldots, g_k \in G \text{ such that } G = \langle g_1, \ldots, g_k \rangle\}.$$

We are going to prove that if $|G| = n$, then $d(G) \leq \log_2 n$. Let

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_r = G$$

be a maximal sequence of subgroups. For each $i \in \{1, \ldots, r\}$ let $g_i \in G_i \setminus G_{i-1}$. It is easily shown that

$$G_i = \langle g_1, \ldots, g_i \rangle$$

for all i. Indeed, if there exists some i such that $G_i \neq \langle g_1, \ldots, g_i \rangle$, then there exists $g \in G_i \setminus \langle g_1, \ldots, g_i \rangle$ and then

$$\langle g_1, \ldots, g_i \rangle \subsetneq \langle G_i, g \rangle \subsetneq G_{i+1}$$

which contradicts the maximality of the sequence of subgroups. In particular, G is generated by r elements.

By Lagrange's theorem,

$$n = |G| = \prod_{i=1}^{r} (G_i : G_{i-1}) \geq 2^r$$

and then $r \leq \lfloor \log_2 n \rfloor$. As G is isomorphic to a subgroup of $\mathbb{S}_n$ by Cayley's theorem, then

$$\begin{aligned} \operatorname{gnu}(n) &\leq \text{number of subgroups of order } n \text{ of } \mathbb{S}_n \\ &\leq \text{number of subgroups of } \mathbb{S}_n \text{ generated by } \lfloor \log_2 n \rfloor \text{ elements} \\ &\leq \text{number of subsets of } \mathbb{S}_n \text{ of } \lfloor \log_2 n \rfloor \text{ elements.} \end{aligned}$$

Since the number of subsets of $\mathbb{S}_n$ of $\lfloor \log_2 n \rfloor$ elements is

$$\binom{n!}{\lfloor \log_2 n \rfloor} \leq (n!)^{\log_2 n}$$

since $\binom{n}{k} \leq n^k$, we conclude that $\operatorname{gnu}(n) \leq n^{n \log_2 n}$. □

In the case of p-groups, it can be shown by elementary methods that

$$\operatorname{gnu}(p^n) \leq p^{\frac{1}{6}(n^3 - n)},$$

see [**4**, Theorem 5.1]. Much more sophisticated bounds are known:

THEOREM 12.41 (Higman–Sims). *If p is a prime number and $n \geq 1$, then*

$$p^{\frac{2}{27} n^3 - O(n^2)} \leq \operatorname{gnu}(p^n) \leq p^{\frac{2}{27} n^3 + O(n^{\frac{8}{3}})}.$$

The proof of the above theorem results from combining the works of Higman [**19**] and Sims [**30**]. A modern presentation can be found in the book [**4**].

In [**20**], Higman conjectured that $\operatorname{gnu}(p^n)$ is a polynomial function of p and p modulo N for a certain finite number of integers N.

CONJECTURE 12.42 (Higman). Let $n \geq 1$. Then there exist N polynomials

$$P_0(X), P_1(X), \ldots, P_{N-1}(X)$$

such that if $p \equiv i \bmod N$, then $\operatorname{gnu}(p^n) = P_i(p)$.

PORC stands for **P**olynomial **O**n **R**esidue **C**lasses.

It is known that the conjecture is true for $n \leq 7$, although the problem remains open for $n \geq 8$. In [**9**], a work of over seventy pages, du Sautoy and Vaughan–Lee constructed a family of groups of order p^{10} suggesting that the PORC conjecture might not be true. Nevertheless, Higman's PORC conjecture remains open.

THEOREM 12.43 (Pyber). *If $n \geq 1$, then*

$$\mathrm{gnu}(n) \leq n^{\frac{2}{27}\mu(n)^2 + O\left(\mu(n)^{\frac{5}{3}}\right)},$$

where $\mu(n)$ is the largest exponent appearing in the prime factorization of n.

The proof appears in [**28**] and in the case of non-solvable groups uses the classification of simple groups. A detailed presentation can be found in the book [**4**] by Blackburn, Neumann, and Venkataraman.

Some topics for final projects

We collect here some topics for final presentations. Some topics can also be used as bachelor's or master's theses.

Formanek's theorem. Kaplansky zero divisors conjecture (Conjecture 6.29) holds for supersolvable groups. This is Formanek's theorem, see Theorem 6.30.

Carter subgroups. The existence of Carter subgroups appears in Theorem 2.35. For the proof of Carter's result, we refer to [**5**].

Itô's theorem. This nice theorem is surprisingly easy to prove. See Theorem 4.16. There is a generalization found by Sysak, see Theorem 4.17.

The Mann subgroup. How the set of sizes of conjugacy classes of a finite group influence the structure of the group? A partial answer goes back to Mann. See Theorem 5.22.

The Chermak–Delgado subgroup. In [**6**], Chermak and Delgado presented a measuring argument for finite groups. They obtained some results about special families of finite groups, and powerful applications to finite simple groups and finite p-groups. See Theorem 12.17.

Hall's subgroups. For finite solvable groups, Hall developed a theory similar to that of Sylow. The proofs presented in Theorems 8.6 and 8.9 (see page 42) use the Schur–Zassenhaus theorems.

Hall's marriage theorem. Given a set of n employees, fill out a list of the jobs each of them would be able to preform. We can give each person the "perfect" job if and only if for every $k \in \{1,\dots,n\}$ the union of any k of the lists contains at least k jobs.

For a proof of the Hall marriage theorem, see [**17**]. The theorem is equivalent to several other powerful theorems in combinatorics. Hall's theorem provides a combinatorial way of solving Exercise 12.27.

The Wielandt automorphism tower theorem. One striking application of subnormality is a beautiful result of Wielandt about the automorphism tower of a finite group with trivial center. See Theorem 8.41.

Gardam's theorem. Let K be a field and G be a torsion-free group. What do the units of $K[G]$ look like? Gardam solved the Kaplansky units problem, answering negatively Question 9.20. See Theorem 9.22 for his solution for fields of characteristic two.

Passman's theorem. There are several interesting open problems in the theory of group algebras. One of these problems is about zero-divisors in group algebras and another one is about group algebras being reduced as rings. Passman's theorem states that these problems are equivalent. See Theorem 9.46.

The Alperin–Kuo theorem. One way to prove the Alperin–Kuo theorem (see Theorem 9.24) is to combine ring-theoretical tools with the transfer homomorphism. The original proof uses group cohomology; see [**1**].

References

[1] J. L. Alperin and T.-n. Kuo. The exponent and the projective representations of a finite group. *Illinois J. Math.*, 11:410–413, 1967.

[2] H. U. Besche, B. Eick, and E. A. O'Brien. The groups of order at most 2000. *Electron. Res. Announc. Amer. Math. Soc.*, 7:1–4, 2001.

[3] H. U. Besche, B. Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[4] S. R. Blackburn, P. M. Neumann, and G. Venkataraman. *Enumeration of finite groups*, volume 173 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2007.

[5] R. W. Carter. Nilpotent self-normalizing subgroups of soluble groups. *Math. Z.*, 75:136–139, 1960/61.

[6] A. Chermak and A. Delgado. A measuring argument for finite groups. *Proc. Amer. Math. Soc.*, 107(4):907–914, 1989.

[7] J. H. Conway, H. Dietrich, and E. A. O'Brien. Counting groups: gnus, moas, and other exotica. *Math. Intelligencer*, 30(2):6–18, 2008.

[8] C. D. H. Cooper. Subgroups of a supersoluble group. *Amer. Math. Monthly*, 78:1007, 1971.

[9] M. du Sautoy and M. Vaughan-Lee. Non-PORC behaviour of a class of descendant p-groups. *J. Algebra*, 361:287–312, 2012.

[10] W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.

[11] D. García-Lucas, L. Margolis, and A. del Río. Non-isomorphic 2-groups with isomorphic modular group algebras. *J. Reine Angew. Math.*, 783:269–274, 2022.

[12] G. Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.

[13] B. J. Gardner and R. Wiegandt. *Radical theory of rings*, volume 261 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 2004.

[14] G. Gonthier, A. Asperti, J. Avigad, and et al. A machine-checked proof of the odd order theorem. In *Interactive theorem proving*, volume 7998 of *Lecture Notes in Comput. Sci.*, pages 163–179. Springer, Heidelberg, 2013.

[15] R. M. Guralnick, M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep. Surjective word maps and Burnside's $p^a q^b$ theorem. *Invent. Math.*, 213(2):589–695, 2018.

[16] M. Hall, Jr. *The theory of groups*. Chelsea Publishing Co., New York, 1976. Reprinting of the 1968 edition.

[17] P. R. Halmos and H. E. Vaughan. The marriage problem. *Amer. J. Math.*, 72:214–215, 1950.

[18] M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001.

[19] G. Higman. Enumerating p-groups. I. Inequalities. *Proc. London Math. Soc. (3)*, 10:24–30, 1960.

[20] G. Higman. Enumerating p-groups. II. Problems whose solution is PORC. *Proc. London Math. Soc. (3)*, 10:566–582, 1960.

[21] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[22] I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[23] N. Itô. On finite groups with given conjugate types. I. *Nagoya Math. J.*, 6:17–28, 1953.

[24] I. Kaplansky. Problems in the theory of rings. In *Report of a conference on linear algebras, June, 1956*, pages 1–3. Nat. Acad. Sci., Washington, DC, 1957. Publ. 502.

[25] M. Le. A divisibility problem concerning group theory. *Pure Appl. Math. Q.*, 8(3):689–691, 2012.

[26] J. Pakianathan and K. Shankar. Nilpotent numbers. *Amer. Math. Monthly*, 107(7):631–634, 2000.

[27] D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.

[28] L. Pyber. Enumerating finite groups of given order. *Ann. of Math. (2)*, 137(1):203–220, 1993.

[29] J.-P. Serre. *Finite groups: an introduction*, volume 10 of *Surveys of Modern Mathematics*. International Press, Somerville, MA; Higher Education Press, Beijing, 2016. With assistance in translation provided by Garving K. Luli and Pin Yu.

[30] C. C. Sims. Enumerating p-groups. *Proc. London Math. Soc. (3)*, 15:151–166, 1965.

[31] N. M. Stephens. On the Feit-Thompson conjecture. *Math. Comp.*, 25:625, 1971.

[32] Y. P. Sysak. Products of almost abelian groups. In *Investigations of groups with restrictions for subgroups (Russian)*, pages 81–85, iii. Akad. Nauk Ukrain. SSR, Inst. Mat., Kiev, 1988.

Index