M1 2021–2022: GROUPS

David Harari

Contents

1. A few reminders

These are mainly reminders from L3, so we will move fairly quickly without going into detail for most of the proofs. We assume that the concepts of groups, subgroups, and group homomorphisms are already known.

1.1. Notation, basic properties

Group laws will in general be given multiplicatively. In particular, the identity element of a group G will most often be denoted 1 and the inverse of an element x denoted x^{-1}. For $n > 0$, we set $x^n = x.x...x$ (n terms), with the

conventions $x^0 = 1$ and $x^{-n} = (x^n)^{-1}$. If the group G is abelian (i.e., commutative), we will sometimes note $+$ the operation, 0 the identity element, and $-x$ the inverse of x, here also known as the *opposite* of x. We can then further write $x - y$ for $x + (-y)$, and nx for $x + x + \ldots + x$ (n terms) when n is a positive integer, with the conventions $0.x = 0$ and $(-n)x = n(-x)$.

Remark 1.1 One should be careful not to use notation like "x/y" if G is non-abelian as it is not clear whether this would mean xy^{-1} or $y^{-1}x$.

Example 1.2 a) The trivial group $G = \{0\}$.

b) $(\mathbf{R}, +)$ and $(\mathbf{R}^*, \times)$ are groups (but not $(\mathbf{R}, \times)$, as the 0 element has no inverse).

The same goes when replacing $\mathbf{R}$ by $\mathbf{C}$ or by any field[1].

c) $G = (\mathbf{Z}/n\mathbf{Z}, +)$, where $n \in \mathbf{N}^*$. This is of order (i.e., of cardinality) n. We will sometimes abbreviate $\mathbf{Z}/n\mathbf{Z}$ to $\mathbf{Z}/n$.

d) If G and H are groups, the set $G \times H$ where $(g, h).(g', h') := (gg', hh')$ is automatically a group too. This generalizes to a (not necessarily finite) family of groups. Here we say that the resulting group is the *direct product* of the original groups.

e) Let E be a set and $\mathcal{S}(E)$ the set of bijections from E to E. Then $\mathcal{S}(E)$, endowed with the composition of functions $\circ$ is a group. When $E = \{1, \ldots, n\}$, we write $\mathcal{S}_n$ for $\mathcal{S}(E)$ and call this the *symmetric group* over n letters (or n elements). Its order is $n!$ and it is non-abelian for $n \geq 3$.

f) Let K be a field. Then the set $\mathrm{GL}_n(K)$ of invertible matrices (n, n) is a group (non-abelian if $n \geq 2$) for multiplication.

Definition 1.3 Suppose $f : G \to G'$ is a group homomorphism. If f is bijective, then f^{-1} is also a homomorphism and we say that f is an *isomorphism* from G to G'. An isomorphism from G to itself is called an *automorphism* of G.

Remark 1.4 a) The set $\mathtt{Aut}G$ of automorphisms of G, endowed with the composition of functions $\circ$ is a subgroup of $\mathcal{S}(G)$. It may not be commutative even if G is (e.g., if $G = \mathbf{Z}/2 \times \mathbf{Z}/2$, this can be seen by observing that $\mathtt{Aut}G$ is isomorphic to $GL_2(\mathbf{Z}/2)$).

b) We will sometimes write $G \simeq H$ to signify that "G is isomorphic to H."

[1] A *field* is a non-zero commutative ring in which every non-zero element has an inverse.

Example 1.5 a) If $a \in \mathbf{R}$, then $x \mapsto ax$ is a homomorphism from $(\mathbf{R}, +)$ to itself. It is an isomorphism if $a \neq 0$, and this remains true when replacing $\mathbf{R}$ with any other field.

b) The function $z \mapsto \exp z$ is a homomorphism which is onto but not one-to-one from $(\mathbf{C}, +)$ to $(\mathbf{C}^*, \times)$.

c) If G is a group and $a \in G$, the function $x \mapsto ax$ ("left translation") is a bijection from G to G, but **not** a homomorphism (except in trivial cases).

d) If G is abelian and $n \in \mathbf{N}^*$, then the function $x \mapsto x^n$ is a homomorphism, but this is not true in general if G is non-abelian. Note also that for any group G, the function $x \mapsto x^{-1}$ is an "antihomomorphism" from G to G, i.e., we have $(xy)^{-1} = y^{-1}x^{-1}$. [2]

e) If E is finite and of cardinality n, we have $\mathcal{S}(E) \simeq \mathcal{S}_n$. For $n \geq 2$, there exists a unique nontrivial homomorphism ε from $\mathcal{S}_n$ to $\{\pm 1\}$ called the *signature*. In particular, the signature of any transposition is -1.

f) Let K be a field. The determinant is a homomorphism from $\mathrm{GL}_n(K)$ to K^*. If E is a K-vector space of dimension n, then $\mathrm{GL}_n(K)$ is isomorphic to the group $(\mathrm{GL}(E), \circ)$ of linear bijective functions from E to E.

We now recall the following result.

Proposition 1.6 *If $f : G \to H$ is a group homomorphism, then the direct image $f(G')$ of a subgroup G' of G and the inverse image $f^{-1}(H')$ of a subgroup H' of H are respectively subgroups of H and G. In particular, the* kernel $\ker f := f^{-1}(\{1\})$ *is a subgroup of G and the* image $\mathrm{Im}\, f := f(G)$ *is a subgroup of H. The homomorphism f is one-to-one if and only if its kernel is made up of the identity element only.*

Example 1.7 a) If $a \in \mathbf{R}$, then $a\mathbf{Z}$ is a subgroup of $(\mathbf{R}, +)$ (all subgroups that are not dense are of this form).

b) The subgroups of $\mathbf{Z}$ are the $n\mathbf{Z}$ with $n \in \mathbf{N}$.

c) Let $n \geq 2$. The kernel of the signature $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$ is a subgroup of $\mathcal{S}_n$ known as the *alternating group* $\mathcal{A}_n$.

d) Let K be a field. The kernel of the determinant $\mathrm{GL}_n(K) \to K^*$ is a subgroup of $\mathrm{GL}_n(K)$ called the *special linear group*, written $\mathrm{SL}_n(K)$.

e) If $(A, +)$ is an abelian group and $n \in \mathbf{N}^*$, then the set $A[n]$ of x in A that satisfy $nx = 0$ is a subgroup of A, called the *n-torsion subgroup.*

[2] In formal terms, it is a homomorphism from G to G^{opp}, where the latter is the group with the same underlying set as G but with group law defined by $x \bullet y = yx$.

The group $A_{\text{tors}} := \bigcup_{n \in \mathbf{N}^*} A[n]$ is also a subgroup [3] of A, called the *torsion subgroup* of A. Note that no good analogue to this notion exists if G is non-abelian.

For example, the torsion subgroup of $(\mathbf{R}, +)$ is $\{0\}$. That of $(\mathbf{R}^*, \times)$ is $\{\pm 1\}$, and that of $\mathbf{C}^*$ is the multiplicative group of all of the roots of unity.

1.2. Generating sets, Lagrange's theorem

Proposition 1.8 *Let G be a group and A a subset of G. Then there exists a smaller (for the inclusion) subgroup H of G that contains A. This is called the* subgroup generated by A *and is written $\langle A \rangle$.*

Proof: It suffices to take for $\langle A \rangle$ the intersection of all subgroups of G containing A. We can also write $\langle A \rangle$ as the set of products $x_1 ... x_n$, where each x_i satisfies: $x_i \in A$ or $x_i^{-1} \in A$ (if A is empty we take $\langle A \rangle = \{1\}$).

□

Remark 1.9 If G is abelian (given additively), it is easier to describe $\langle A \rangle$ as being simply the set of $\sum_{i=1}^{m} n_i a_i$ with $n_i \in \mathbf{Z}$ and $a_i \in A$ (with m an arbitrary integer), i.e., the set of $\sum_{a \in A} n_a a$, where $(n_a)_{a \in A}$ is an almost zero family of integers (that is: all but finitely many n_a are zero). Be careful as this does not extend to cases where A is non-abelian (e.g., we cannot simplify an expression like xyx in non-abelian groups).

Definition 1.10 Let G be a group and $g \in G$. The *order* of g is the smallest positive integer $n > 0$ (if it exists) such that $g^n = 1$. If $g^n \neq 1$ for all $n > 0$, we say that g has infinite order. The order of g is also the cardinality of the subgroup $\langle g \rangle$ generated by g.

Recall in particular the following result.

Proposition 1.11 *Let G be a group and $g \in G$. If $\langle g \rangle$ is infinite, it is isomorphic to $\mathbf{Z}$. If its cardinality is n, it is isomorphic to $\mathbf{Z}/n\mathbf{Z}$.*

Definition 1.12 A group is said to be *cyclic* if it can be generated by one element, whether or not the group is finite. In particular, infinite cyclic groups are isomorphic to $\mathbf{Z}$ while finite ones are isomorphic to $\mathbf{Z}/n\mathbf{Z}$, where n is the group's cardinality.

[3] Warning: In general the union of subgroups is not a subgroup; this works here because an x which satisfies $mx = 0$ or $nx = 0$ satisfies $(mn)x = 0$.

The following result is of great importance.

Theorem 1.13 (Lagrange's theorem) *Let G be a finite group. Then the order of any subgroup H of G divides the order of G. In particular, the order of any element of G is finite and divides the order of G.*

(The theorem is proved by looking at the left cosets aH for $a \in G$, which correspond to a partition of G. However, the cardinality of each left coset aH is the same as that of H since left translations are bijections of G onto G).

Proposition 1.14 *Let $G = \mathbf{Z}/n\mathbf{Z}$ and suppose that d is a positive divisor of n. Then G has one (and one only) subgroup of order d. This subgroup C_d is cyclic and of order d (and thus isomorphic to $\mathbf{Z}/d\mathbf{Z}$).*

Proof: First, notice that $C_d := \{\bar{0}, \overline{n/d}, \ldots, \overline{(d-1)n/d}\}$ is a subgroup of order d of G. If now H is a subgroup of order d of G, Lagrange's theorem says that any element x of H satisfies $dx = 0$, or in other words, $H \subset C_d$. As H and C_d are both of cardinality d, it follows that $H = C_d$.

□

Example 1.15 a) The group $(\mathbf{Z}^n, +)$ is generated by the family

$$(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1).$$

b) The symmetric group $\mathcal{S}_n$ is generated by the set of transpositions.

c) For $n \geq 2$, the orthogonal group $O_n(\mathbf{R})$ is generated by the set of *reflections* (=orthogonal symmetries with respect to a hyperplane), and for $n \geq 3$ the special orthogonal group $SO_n(\mathbf{R}) := O_n(\mathbf{R}) \cap \mathrm{SL}_n(\mathbf{R})$ is generated by the set of orthogonal symmetries with respect to a subspace of codimension 2.

d) The group $(\mathbf{Q}, +)$ cannot be generated by a finite subset (Exercice!).

1.3. Normal subgroups, quotient groups.

Let us first recall a proposition whose proof is immediate.

Proposition 1.16 *Let G be a group and $g \in G$. Then the function* $\mathrm{int}\, g : G \to G$, $h \mapsto ghg^{-1}$ *is an automorphism of G, known as the inner automorphism associated with g. The function $g \mapsto \mathrm{int}\, g$ is a group homomorphism from G to $(\mathtt{Aut}G, \circ)$.*

Definition 1.17 A subgroup H of G is said to be *normal* if it is invariant with respect to any inner automorphism, i.e., for any g in G and all h in H, we have $ghg^{-1} \in H$. If so, we write: $H \lhd G$.

Remark 1.18 a) $H \lhd G$ is the same thing as $gHg^{-1} = H$ for any g in G (start with $gHg^{-1} \subset H$, change g into g^{-1}, left multiply by g and right multiply by g^{-1}).

b) If G is abelian, all of its subgroups are normal.

c) $\{1\}$ and G are always normal subgroups of G.

d) Careful: the notion of normal subgroup is relative (e.g., H is always normal when seen as a subgroup of itself).

Example 1.19 a) If $f : G \to G'$ is a group homomorphism and $H' \lhd G'$, then $f^{-1}(H')$ is a normal subgroup of G. In particular $\ker f$ is a normal subgroup of G. If $H \lhd G$, then $f(H)$ is a normal subgroup of $f(G)$ (but not of G' in general). The intersection of two normal subgroups of G is a normal subgroup of G.

b) Let $n \geq 2$. Then $\mathcal{A}_n$ is a normal subgroup of $\mathcal{S}_n$ given that it is the kernel of the signature.

c) If K is a field, then $\mathrm{SL}_n(K)$ is a normal subgroup of $\mathrm{GL}_n(K)$ (given that it is the kernel of the determinant map).

d) Suppose $n \geq 3$ and H is the subgroup of $\mathcal{S}_n$ made up of the identity and a transposition $\tau = (a, b)$. Then if $\sigma \in \mathcal{S}_n$, we have $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))$, so H is not a normal subgroup of $\mathcal{S}_n$ (choose σ such that $\sigma(a) = c$ with c different from a and b).

Remark 1.20 Be careful, because $\lhd$ is not transitive; it is possible to have $K \lhd H \lhd G$ without $K \lhd G$ being true. For example, let $V_4 \subset \mathcal{S}_4$ be the set made up of the identity and the three double-transpositions $(a, b)(c, d)$ where $\{a, b, c, d\} = \{1, 2, 3, 4\}$. Then V_4 is a normal subgroup of $\mathcal{S}_4$, isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and contains subgroups of order 2 that are not normal subgroups in $\mathcal{S}_4$.

Definition 1.21 A subgroup H of G is said to be *characteristic* if for any $\varphi \in \mathtt{Aut}G$, we have $\varphi(H) \subset H$ (in this case, we have in particular that $H \lhd G$).

For example, the group $\mathcal{A}_3$ is a characteristic subgroup of $\mathcal{S}_3$ since any automorphism of $\mathcal{S}_3$ has to map a 3-cycle onto an element of order 3, which is in fact another 3-cycle. We will see, further on, two general examples of characteristic subgroups of a group G: its *center* and its *commutator subgroup*. We will also see that $\mathcal{A}_n$ is the commutator subgroup of $\mathcal{S}_n$.

Remark 1.22 If K is characteristic in H and H is characteristic in G, it is easy to show (Exercise!) that K is characteristic in G.

Recall that if H is a subgroup G, then the left cosets G/H (resp. right cosets $H \setminus G$) are the sets aH (resp. Ha) for $a \in G$; The set of left cosets is the *quotient set* of G for the equivalence relation $x \sim y$ if $x^{-1}y \in H$ (resp. $xy^{-1} \in H$).

Theorem 1.23 *Let G be a group and H a normal subgroup of G. Then:*

a) For any a in G, we have $aH = Ha$ and thus $G/H = H \setminus G$.

b) There exists a unique group structure on G/H such that the canonical projection $p : G \to G/H$ (which associates each a with the coset $\bar{a} = aH = Ha$) is a group homomorphism. The group G/H thus obtained is called the quotient group of G by H.

Proof: a) By the definition of a normal subgroup, we have $aHa^{-1} \subset H$ and $a^{-1}Ha \subset H$, and thus $aH \subset Ha$ and $Ha \subset aH$.

b) The group law on G/H must necessarily be defined by $\bar{a}\bar{b} = \overline{ab}$. First, let us show that this law is well defined, i.e., that $\bar{a}\bar{b}$ does not depend on which a and b are chosen. If $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$, from (a) we have that $a' = h_1 a$ and $b' = bh_2$ with h_1, h_2 in H, and thus $a'b' = h_1(ab)h_2$. Hence, $a'b' \in H(abh_2) = (abh_2)H$ according to (a), but the latter set is no other than $(ab)H$ since $h_2 \in H$. We therefore obtain $a'b' \sim ab$, as required.

The fact that the group law is well defined then comes immediately from the fact that p is onto and from the formula $p(xy) = p(x)p(y)$ for all x, y in G.

□

Remark 1.24 a) The identity element of G/H is $\bar{1} = H$.

b) If G is abelian, we can thus take the quotient with respect to any subgroup, but it is easy to see that the theorem is always false if H is not a normal subgroup of G. ("G/H is just a set"), seeing as the required property implies that H is the kernel of the group homomorphism p.

c) The group $\mathbf{Z}/n\mathbf{Z}$ is the quotient group of $\mathbf{Z}$ by the subgroup $n\mathbf{Z}$.

d) If H is a subgroup of a group G, there is a bijection between G/H and $H \setminus G$ via $aH \mapsto Ha^{-1}$. When these cardinalities are finite, we say that H is a *finite index* subgroup of G with index $[G : H]$ equal to $\#G/\#H$ when G is finite.

Theorem 1.25 (Factorization theorem) *Let $f : G \to G'$ be a group homomorphism. Then there exists a unique group homomorphism $\tilde{f} : G/\ker f \to$*

G' such that $f = \tilde{f} \circ p$. Furthermore, $\tilde{f}$ is one-to-one with image $\operatorname{Im} f$, i.e., $G/\ker f \simeq \operatorname{Im} f$ ("First isomorphism theorem"). In particular, when G is finite, we have

$$\#G = \#\ker f \#\operatorname{Im} f.$$

Proof (sketch): The function $\tilde{f}$ must be defined by $\tilde{f}(\bar{a}) = f(a)$, where $\bar{a}$ is the image of a in G/H. This definition makes sense because if $\bar{a} = \bar{b}$, then $a = bn$ with $n \in \ker f$, and thus $f(a) = f(b)f(n) = f(b)$. The other properties then follow immediately.

□

Remark 1.26 If N is a normal subgroup of G inside $\ker f$, then f can also be factorized by a homomorphism $\tilde{f} : G/N \to G'$ with image $\operatorname{Im} f$, though $\tilde{f}$ is not one-to-one.

Theorem 1.27 ("Second and third isomorphism theorems")

Let G be a group. Suppose that H is a normal subgroup of G, and note $p : G \to G/H$ the canonical projection. Then:

a) The subgroups of G/H are the same as those of N/H, where N is a subgroup of G containing H. Furthermore, $N/H \lhd G/H$ if and only if $N \lhd G$.

b) Let K be a subgroup of G. Set $KH = \{kh, k \in K, h \in H\}$ (with similar notation for HK). Then we have $KH = HK$, and this set is a subgroup of G which contains H.

c) For any subgroup K of G, the subgroup $p(K)$ of G/H is the same as the subgroup KH/H. The latter is isomorphic to $K/K \cap H$ ("Second isomorphism theorem").

d) Let N be a normal subgroup of G that contains H. Then the group $(G/H)/(N/H)$ is isomorphic to the quotient group G/N ("Third isomorphism theorem").

Thus, in G/H "we get a subgroup if we shrink G and a quotient group if we enlarge H".

Proof: a) The proof is immediate that if N is a subgroup of G containing H, then H (which is normal in G) is *a fortiori* normal in N, and thus N/H is a subgroup of G/H. Inversely, if A is a subgroup of G/H, then $N := p^{-1}(A)$ is a subgroup of G containing H (since A contains the identity element of G/H), and we indeed have $A = p(N) = N/H$ since p is onto. If $A \lhd G/H$, its inverse image N is a normal subgroup of G, and if $N \lhd G$, then $A = p(N)$ is indeed normal in $p(G) = G/H$.

b) The equality $KH = HK$ results from the identities (valid for $k \in K, h \in H$): $kh = (khk^{-1})k$ and $hk = k(k^{-1}hk)$ with $khk^{-1} \in H$, $k^{-1}hk \in H$ seeing as $H \lhd G$. We have thus $1 = 1.1 \in HK$; if $u_1, u_2 \in KH$, we can write $u_1 = k_1h_1$ and $u_2 = h_2k_2$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then $u_1u_2 = k_1h_3k_2$ with $h_3 = h_1h_2 \in H$; as $h_3k_2 \in HK = KH$, we can write $h_3k_2 = k_3h_4$ with $k_3 \in K$ and $h_4 \in H$, which gives that $u_1u_2 = (k_1k_3)h_4 \in KH$. Finally, if $u = kh \in KH$, then $u^{-1} = h^{-1}k^{-1} \in HK = KH$. Thus KH is indeed a subgroup of G.

c) Let $u = kh \in KH$. Then we have $p(u) = p(k) \in p(K)$ since $p(h)$ is the identity element of G/H, and thus $KH/H \subset p(K)$. Inversely, any element of $p(K)$ is of the form $\bar{k}$ with $k \in K \subset KH$, and thus obviously in KH/H. Now let $\varphi : K \to KH/H$ be the group homomorphism defined by $\varphi(k) = \bar{k} = p(k)$. Its kernel is clearly $K \cap H$ since $\ker p = H$. As $p(K) = KH/H$, we see that φ is onto, and the factorization theorem then gives that $K/K \cap H \simeq KH/H$.

d) Let $\psi : G/H \to G/N$ be the group homomorphism defined by $\psi(\bar{g}) = \tilde{g}$, where $\tilde{g}$ refers to the image of g in G/N. This definition is meaningful because if g and g' are elements in G with $\bar{g} = \bar{g}'$, then $g^{-1}g' \in H \subset N$ and thus $\tilde{g} = \tilde{g}'$. We see immediately that ψ is onto with kernel N/H, and the result follows with the help of the factorization theorem. □

Remark 1.28 The special case of abelian groups $(A, +)$ is already interesting here: if B is a subgroup of A, then the subgroups of A/B are the C/B, where C is a subgroup of A containing B. More generally, the image in A/B of a subgroup D of A is $(D + B)/B \simeq D/(B \cap D)$.

1.4. The center and the commutator subgroup

Definition 1.29 Let G be a group. The *center* Z of G is the set of elements x in G which satisfy $xy = yx$ for all y in G.

Example 1.30 a) If K is a field, the center of $GL_n(K)$ is the subgroup of $\lambda I_n, \lambda \in K^*$.

b) For $n \geq 3$, the center of $\mathcal{S}_n$ is the identity element only, resulting from the fact that if $\tau = (a, b)$ is a transposition and $\sigma \in \mathcal{S}_n$, then $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))$, and thus σ does not commute with τ upon choosing a such that $\sigma(a) := c$ (c different to a), and then b different to a and c (which is possible to do for any σ that is not the identity, so long as $n \geq 3$).

By defintion, Z is the kernel of the homomorphism int : $G \to \mathtt{Aut}G$ and thus $Z \lhd G$. It is then immediate that Z is a characteristic subgroup of G.

Definition 1.31 Let G be a group and x and y two of its elements. The *commutator* of x and y is defined as the element $[x, y] := xyx^{-1}y^{-1}$. The commutator subgroup of G is by definition the subgroup **generated** by the commutators.[4] We denote this subgroup $D(G)$.

$D(G)$ is of interest because of the following proposition.

Proposition 1.32 *The subgroup $D(G)$ is characteristic (and indeed normal) in G. The quotient $G/D(G)$ is abelian, and $D(G)$ is the smallest subgroup of G with this property. We note $G^{\text{ab}} := G/D(G)$ (i.e., G^{ab} "abelianizes" G).*

The abelianization of G is therefore the "largest abelian quotient" of G in the following sense: if G/H is another abelian quotient, then G/H is a quotient of G^{ab} (via the third isomorphism theorem).

Proof: If φ is an automorphism of G, then we have $\varphi([x, y]) = [\varphi(x), \varphi(y)]$, from which $\varphi(D(G)) \subset D(G)$ and $D(G)$ is characteristic. By the definition of a quotient, any commutator of $G/D(G)$ is trivial, so $G/D(G)$ is abelian. Finally, if $H \lhd G$ is a subgroup for which G/H is abelian, then we have $\overline{xyx^{-1}y^{-1}} = \bar{e}$ in G/H for any x and y from G, therefore $[x, y] \in H$; hence H contains $D(G)$ since it contains all commutators.[5] □

For example, $D(G) = \{1\}$ if and only if G is abelian and $D(\mathcal{S}_3) = \mathcal{A}_3$; in effect, we see immediately that the signature of a commutator is 1, thus $D(\mathcal{S}_3) \subset \mathcal{A}_3$; but $\mathcal{S}_3$ is not commutative so $D(\mathcal{S}_3)$ is not trivial, thus $D(\mathcal{S}_3) = \mathcal{A}_3$ is the only possibility via Lagrange's theorem, given that $\mathcal{A}_3$ has a cardinality of 3.

We will see later that for $n \geq 3$, we have $D(\mathcal{S}_n) = \mathcal{A}_n$ and thus $\mathcal{S}_n^{\text{ab}} \simeq \mathbf{Z}/2\mathbf{Z}$.

2. Finite groups

2.1. Group actions, the class formula

Definition 2.1 Let G be a group and X a set. We say that G *acts* on X if we are given a map $G \times X \to X$, $(g, x) \mapsto g.x$, such that the following holds:

[4] Warning: The set of commutators is not in general a subgroup, though it can be hard to construct counterexamples.

[5] Conversely, if H is a subgroup that contains $D(G)$, then H is automatically normal since if $h \in H$ and $g \in G$, then $(ghg^{-1})h^{-1} \in D(G) \subset H$, from which $ghg^{-1} \in H$; it immediately follows that G/H is abelian.

- For any g and g' in G and any x in X, we have $g.(g'.x) = (gg').x$
- For any x in X, we have $1.x = x$

Remark 2.2 a) In particular, for any g, $x \mapsto g.x$ is a bijection from X to X, with inverse $x \mapsto g^{-1}.x$. An equivalent definition consists in providing a homomorphism $\Phi : G \to (\mathcal{S}(X), \circ)$, setting $g.x = (\Phi(g))(x)$.

b) The above definition corresponds to *left action*. We can also talk about *right action*, i.e., $(g, x) \mapsto x.g$, satisfying $x.(gg') = (x.g).g'$. This corresponds to providing an antihomomorphism from G to $\mathcal{S}(X)$ in the place of a homomorphism.

Example 2.3 a) G can act on itself by *left translation* via $g.x := gx$. Similarly, any subgroup H of G can act on G by left translation.

b) G can act on itself by *conjugation*: $g.x := gxg^{-1}$. Here the image of G in $\mathcal{S}(G)$ is furthermore contained in $\mathtt{Aut}G$ (which was not true in the previous example). We then say that G *acts by automorphisms*.

c) $\mathcal{S}_n$ acts on $\{1, \ldots, n\}$ by $\sigma.x = \sigma(x)$.

d) If H is a subgroup of G, G acts on the left cosets G/H by $g.(aH) = (ga)H$.

Definition 2.4 Given a group action for a group G on a set X,

- the *orbit* of an element x in X is the set of $g.x$, $g \in G$. Orbits are equivalence classes in X as defined by : $x \sim y$ if and only if there exists $g \in G$ such that $y = g.x$. If only one orbit exists, we say that G acts *transitively* on X.
- the *stabilizer* of an element x in X is the subgroup Stab_x of elements g in G satisfying $g.x = x$. This subgroup is not in general normal in G. We say that an action is *faithful* if the only element of G that stabilizes all elements of X is the neutral element 1 of G, and *free* if all stabilizers are $\{1\}$ (a much stronger condition).

Example 2.5 a) If H is a subgroup of G, the action of H on G by left translation is free, and the orbits are nothing but the right cosets with respect to H. If G is finite and of order n, we get in particular that there exists a one-to-one homomorphism (G acting on itself) from G to $\mathcal{S}(G) \simeq \mathcal{S}_n$ (Cayley's theorem).

b) The action of $\mathcal{S}_n$ on $\{1, \ldots, n\}$ is transitive, and all stabilizers are isomorphic to $\mathcal{S}_{n-1}$.

c) The action of G on G/H seen earlier is transitive. The following proposition says that this is in some sense the "usual" kind of transitive action.

Proposition 2.6 *Given a group action for a group G on a set X and $x \in X$, we define a bijection from G/Stab_x to the orbit $\omega(x)$ of x via : $\bar{g} \mapsto g.x$. In particular, if G is finite, we have $\#\,\omega(x) = \#G/\#\mathrm{Stab}_x$ (the cardinality of $\omega(x)$ thus divides G). Then, if the action is transitive, the action of G identifies with the action of G on G/Stab_x by left translation.*

Proof: First, the function $\varphi : \bar{g} \mapsto g.x$ from G/Stab_x to X is well defined because as $\bar{g} = \bar{g}'$, we have $g' = g.h$ with $h \in \mathrm{Stab}_x$, and thus $g'.x = g.(h.x) = g.x$. Also, it is onto by the definition of an orbit. Then, if $g.x = g'.x$, we have $(g'^{-1}g).x = x$, i.e., $g'^{-1}g \in \mathrm{Stab}_x$, or $\bar{g}' = \bar{g}$ in G/Stab_x.

□

Corollary 2.7 (The class formula) *Let G be a finite group that acts on a finite set X. Let Ω be the set of orbits, and denote $\#\mathrm{Stab}_\omega$ the cardinality of the stabilizer of x for x in the orbit ω (which is independent of the choice of x in Ω thanks to the previous proposition). Then,*

$$\#X = \sum_{\omega \in \Omega} \frac{\#G}{\#\mathrm{Stab}_\omega}.$$

Proof: Since the orbits form a partition of X, the result is immediate thanks to the previous proposition. Nevertheless, the consequences of this result are far from trivial (as we will see later!).

□

Remark 2.8 The formula remains valid if G is infinite by replacing $\frac{\#G}{\#\mathrm{Stab}_\omega}$ by the index $[G : \mathrm{Stab}_\omega]$ (which is finite if X is finite, via proposition 2.6).

Theorem 2.9 (Burnside's formula) *Let G be a finite group acting on a finite set X. For any $g \in G$, note $\mathrm{Fix}\, g$ the subset of X made up of the fixed points of g (that is: the set of $x \in X$ such that $g.x = x$). Then*

$$\sum_{x \in X} \frac{1}{\#\,\omega(x)} = \frac{1}{\#G} \sum_{g \in G} \#(\mathrm{Fix}\, g).$$

This number is also equal to the number of orbits.

Proof: Let E be the set of pairs (g,x) of $G \times X$ that satisfy $g.x = x$. Then, its cardinality is $\sum_{g\in G} \#(\mathrm{Fix}\, g)$, as for each g in G we have $\mathrm{Fix}\, g$ elements x of X such that $(g,x) \in E$. However, this cardinality is also $\sum_{x\in X} \#\mathrm{Stab}_x = \sum_{x\in X} \frac{\#G}{\#\,\omega(x)}$ since for each $x \in X$, we have $\#\mathrm{Stab}_x = \frac{\#G}{\#\,\omega(x)}$ elements g in G for which $(g,x) \in E$. Hence the formula. Also, if Ω is the set of orbits, we have

$$\sum_{x\in X} \frac{1}{\#\,\omega(x)} = \sum_{\omega\in\Omega} \sum_{x\in\omega} \frac{1}{\#\omega} = \sum_{\omega\in\Omega} 1 = \#\Omega.$$

□

2.2. p-groups and Sylow's theorems

Definition 2.10 Suppose p is prime. A *p-group* is a group of cardinality p^n, where n is an integer[6].

Proposition 2.11 *Let G be a nontrivial p-group. Then :*

a) The center Z of G is nontrivial.

b) If G has cardinality p or p^2, then it is abelian.

Proof: a) We begin by having G act on itself by conjugation. There are $\#Z$ orbits made up of only one element each, and the cardinalities of the other orbits divide $p^n := \#G$ (not equal to 1), and are thus divisible by p. Hence p^n (with $n > 0$) is the sum of the cardinality of Z and a multiple of p, so p divides $\#Z$.

b) If G is of cardinality p, then the order of any nontrivial element of G divides p and is thus of order p, so G is cyclic. Now suppose that G is of cardinality p^2. If G is non-abelian, the cardinality of Z would be p from (a), and thus G/Z would be cyclic (since it is of cardinality p). However, a contradiction occurs via the following lemma :

Lemma 2.12 *Let G be a group with center Z for which G/Z is cyclic. Then G is abelian.*

The lemma can be proved by selecting a generator $\bar{a}$ of G/Z. Then, any element g of G can be written $g = a^m z$ with $z \in Z$, and it immediately follows that the two elements of G commute.

□

[6]Some authors consider that the trivial group is not a p-group; we prefer the convention that it is, thus allowing us to affirm that a subgroup of a p-group is always a p-group.

We now move on to Sylow's theorems, which arise from the following question : Given a finite group G and an integer n that divides its cardinality, can we find a subgroup of order n? In general the answer is no (e.g., $\mathcal{A}_4$ is of cardinality 12 but has no subgroup of order 6. Exercise!), but in the special case of p-subgroups, we will see that the answer is affirmative.

Definition 2.13 *Let p be prime and let G be a group of cardinality $n = p^\alpha m$ with $\alpha \in \mathbf{N}, m \in \mathbf{N}^*$. Suppose that p is not a divisor of m. A Sylow p-subgroup (or p-Sylow for short) is then defined as a subgroup H of cardinality p^α.*

In other words, a p-Sylow is a p-subgroup of G whose index is prime to p (this notion is of interest if p divides the order of G; otherwise a p-Sylow is simply the trivial group).

Theorem 2.14 (Sylow's first theorem) *Let G be a finite group and p a prime number. Then G contains at least one Sylow p-subgroup.*

The proof is based on two lemmas, which are of interest in their own right.

Lemma 2.15 *Let H be a subgroup of G. If G contains a p-Sylow S, then there exists $a \in G$ such that $aSa^{-1} \cap H$ is a p-Sylow of H.*

This lemma shows that in order to prove the Theorem for a group H, it is sufficient to prove it for some group G containing H as a subgroup.

Lemma 2.16 *Let $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (field with p elements) and $G_p := \mathrm{GL}_n(\mathbf{F}_p)$ with $n \in \mathbf{N}^*$. Then G_p has a p-Sylow.*

Sylow's first theorem follows easily from these lemmas. In effect, all that remains to be proved is that G is isomorphic to a subgroup of G_p. To this end, note that G is isomorphic to a subgroup of $\mathcal{S}_n$ by Cayley's theorem, and $\mathcal{S}_n$ embeds into G_p by applying the permutation σ to the matrix M_σ, mapping the vector e_i to $e_{\sigma(i)}$, where $(e_1, \ldots, e_n)$ is the canonical basis. [7] It therefore only remains to prove the two lemmas.

[7] Note that if we permute the coordinates instead of the basis vectors, we get an anti-homomorphism rather than a homomorphism.

Proof of lemma 2.15 : The group H acts on the left cosets G/S via $(h, aS) \mapsto (ha)S$. We see immediately that the stabilizer $\mathrm{Stab}_H(aS)$ of aS for this action is $aSa^{-1} \cap H$. Each of these $\mathrm{Stab}_H(aS)$ is a p-group, so it suffices to show that one of them has an index in H that cannot be divided by p. However, this index $\frac{\#H}{\#\mathrm{Stab}_H(aS)}$ is also the cardinality of the orbit $\omega_H(aS)$. As p does not divide the cardinality of the set G/S (since S is a p-Sylow of G), the result comes from the fact that the orbits form a partition of G/S.

□

Proof of lemma 2.16 : First we calculate the cardinality of G_p. This is the same as the number of bases in the $\mathbf{F}_p$-vector space $\mathbf{F}_p^n$ (indeed, if $\mathcal{B}$ is such a basis, there is one and only one element of G_p that maps the canonical basis to $\mathcal{B}$), which is equal to

$$(p^n - 1)(p^n - p)...(p^n - p^{n-1}).$$

Essentially, we have $p^n - 1$ choices for the choice of the first basis vector (any non-zero vector e_1), then $p^n - p$ choices for the second (any vector that is not a multiple of e_1), etc. As a result, a p-Sylow of G_p is of cardinality $p^{1+2+...+n-1} = p^{n(n-1)/2}$, and the set of upper triangular matrices with 1s on the diagonal is a subgroup of G_p with this cardinality.

□

Remark 2.17 As an exercise, it can be shown that a group of cardinality $p^\alpha m$, where p is not a divisor of m, contains subgroups of order p^i for all $i \leq \alpha$ (hint: start with a p-group and use induction on the cardinality, treating abelian and non-abelian G cases separately).

The following theorem looks at the conjugation of p-Sylows.

Theorem 2.18 (Sylow's second theorem) *Let G be a finite group of cardinality $n = p^\alpha m$ where p does not divide m. Then :*

a) If $H \subset G$ is a p-group, there exists a p-Sylow of G that contains it.

b) If S and S' are two p-Sylows of G, then they are conjugate (i.e., there exists $g \in G$ such that $S' = gSg^{-1}$). Furthermore, the number k of p-Sylows divides n.

c) k is congruent to 1(mod p), thus k divides m.

Proof: a) According to Sylow's first theorem, there exists at least one p-Sylow of G. Lemma 2.15 then says that there exists $a \in G$ such that $aSa^{-1} \cap H$ is a p-Sylow of H, i.e., $aSa^{-1} \cap H = H$ since H is a p-group. Thus H is contained in aSa^{-1}, a p-Sylow of G.

b) If H is a p-Sylow of G, we have furthermore that $H = aSa^{-1}$ in cardinality, thus any p-Sylow of G is conjugate to S. Hence let G act by conjugation on the set X of p-Sylows. As there is only one orbit, its cardinality k (which divides that of G via proposition 2.6) is the same as X, i.e., the number of p-Sylows.

c) Let S be a p-Sylow of G, and have S act on X by conjugation. Let X^S be the set of fixed points of this action (i.e., the orbits consisting of one single element) and Ω' the set of the other orbits. The class formula is given by

$$k = \#X^S + \sum_{\omega \in \Omega'} \#\omega.$$

The cardinality of the orbits found in Ω' divides the cardinality of S (which is a power of p) and is not equal to 1; thus, it is divisible by p. To conclude, it therefore suffices to show that there is only one orbit that is made up of one point only (that of S), i.e., if T is a p-Sylow of G such that $sTs^{-1} = T$ for any s in S, then $S = T$.

To show this, we introduce the subgroup N of G generated by S and T. Clearly S and T are p-Sylows of N and therefore conjugate by an element of N via (b). But T is normal in N via the fact that $sTs^{-1} = T$ for any s in S; in effect, the set of $g \in G$ satisfying $gTg^{-1} = T$ is clearly a subgroup of G (called the *normalizer* of T), and we now know that it contains T and S, and thus also the subgroup N generated by them. Hence, $T = S$. [8]

□

An important special case is when m has no divisor $\neq 1$ which is congruent to 1 modulo p. Then G has a unique p-Sylow, which is therefore normal. For example, a group of order 63 is not *simple*, i.e., it has a normal subgroup other than itself and the trivial group; indeed its number k of 7-Sylows must divide 9 and be congruent to 1 modulo 7, and therefore $k = 1$, which implies that the unique 7-Sylow is normal. The same argument works for a group of order 255.

[8] This style of reasoning is called "Frattini's argument".

2.3. Further details on $\mathbf{Z}/n\mathbf{Z}$

We start with the following elementary proposition, which we recall without proof :

Proposition 2.19 *Let $n \in \mathbf{N}^*$, $s \in \mathbf{Z}$. Then the following properties are equivalent:*

i) s and n are coprime.

ii) $\bar{s}$ generates the additive group $\mathbf{Z}/n\mathbf{Z}$.

iii) $\bar{s}$ belongs to the group of units $(\mathbf{Z}/n\mathbf{Z})^*$ in the ring $\mathbf{Z}/n\mathbf{Z}$.

Care should be taken not to confuse additive and multiplicative structures (e.g., do not replace (iii) with "$\bar{s}$ generates $(\mathbf{Z}/n\mathbf{Z})^*$", which is trivially false for example for $s = 1$; we will see that the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$ is not cyclic in general, e.g., for $n = 8$). Also be careful not to write "x and n are coprime" for an element x in $\mathbf{Z}/n\mathbf{Z}$ (instead of "s and n are coprime", where s is an integer such that $\bar{s} = x$), the notion of coprime elements having no meaning in a ring with zero divisors.

We are now going to specify a little the structure of $(\mathbf{Z}/n\mathbf{Z})^*$ and its connection with $\mathtt{Aut}((\mathbf{Z}/n\mathbf{Z}, +))$. For any $n \in \mathbf{N}^*$, we denote $\varphi(n)$ *Euler's totient function* of n, i.e., the number of integers x in $[1, n]$ which are prime to n.

Proposition 2.20 *Let $n \in \mathbf{N}^*$, and write n factorized as powers of distinct primes p_i: $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Then:*

a) The cardinality of $(\mathbf{Z}/n\mathbf{Z})^*$ is $\varphi(n)$. For p prime, we have $\varphi(p) = p-1$, and more generally $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ if $\alpha \geq 1$.

b) The group $\mathtt{Aut}(\mathbf{Z}/n\mathbf{Z})$ of automorphisms of the additive group[9] $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$.

c) We have a ring isomorphism

$$\mathbf{Z}/n\mathbf{Z} \simeq \prod_{i=1}^{r} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$$

and a group isomorphism

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^*.$$

d) We have $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$.

[9] And not of the ring; the only automorphism of the ring $(\mathbf{Z}/n\mathbf{Z})$ is the identity, seeing as $\bar{1}$ has to be mapped to $\bar{1}$.

Proof: (a) is a result of the previous proposition, and the fact that integers in $[1, p^\alpha]$ that are not prime to p are the multiples of p.

b) It is immediate that the function Φ from the group $((\mathbf{Z}/n\mathbf{Z})^*, \times)$ to the group $(\mathtt{Aut}(\mathbf{Z}/n\mathbf{Z}), \circ)$ which maps a to $x \mapsto ax$ is a group homomorphism. The latter is one-to-one because if $\Phi(a)$ is the identity, then $ax = x$ for all x, so $a = 1$ by taking $x = \bar{1}$. It is also onto because if $\varphi \in \mathtt{Aut}(\mathbf{Z}/n\mathbf{Z})$, then by setting $a = \varphi(\bar{1})$, we get that for any x in $\mathbf{N}$, $\varphi(\bar{x}) = \varphi(1 + \ldots + 1)$ (x terms), so $\varphi(\bar{x}) = a\bar{x}$. Also, $a \in (\mathbf{Z}/n\mathbf{Z})^*$ since $\bar{1}$ must be the image of some element of $\mathbf{Z}/n\mathbf{Z}$ by φ.

c) The map from $\mathbf{Z}/n\mathbf{Z}$ to $\prod_{i=1}^r \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$ that sends $\bar{x}$ to $(x_i)_{1 \leq i \leq r}$, where x_i is the class of x mod $p_i^{\alpha_i}$ is clearly a ring homomorphism. The latter is one-to-one because if x can be divided by all of the $p_i^{\alpha_i}$, it can also be divided by their product n since they are pairwise coprime. As $\mathbf{Z}/n\mathbf{Z}$ and $\prod_{i=1}^r \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$ have the same cardinality, this map is also onto[10]. The second assertion of (c) can be seen immediately by noting that isomorphic rings have isomorphic groups of units.

d) Follows directly from (a) and (c).

□

To go further, we would now like to determine the structure of $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ when p is prime and $\alpha \in \mathbf{N}^*$. We begin with the $\alpha = 1$ case.

Theorem 2.21 *Le K be a field*[11] *and G a finite subgroup of the multiplicative group K^*. Then G is cyclic.*

Proof: We will use the following lemma in the proof :

Lemma 2.22 *Let $n \in \mathbf{N}^*$. Then,*

$$n = \sum_{d|n} \varphi(d).$$

This lemma immediately follows from proposition 1.14: the elements of order d in $\mathbf{Z}/n\mathbf{Z}$ are necessarily in the unique subgroup C_d of $\mathbf{Z}/n\mathbf{Z}$ of cardinal d; but since C_d is isomorphic to $\mathbf{Z}/d\mathbf{Z}$, it contains $\varphi(d)$ elements of order d, so in fact $\mathbf{Z}/n\mathbf{Z}$ contains $\varphi(d)$ elements of order d; the lemma follows after sorting the elements of $\mathbf{Z}/n\mathbf{Z}$ by their order.

[10] This is one way to formulate the *Chinese remainder theorem.*

[11] Remember that we impose that the multiplication in K is commutative; otherwise this theorem is false, since e.g., the quaternion algebra $\mathbf{H}$ over $\mathbf{C}$ contains a non-abelian subgroup of $\mathbf{H}^*$ of order 8.

We now return to the proof of theorem 2.21. Let n be the cardinality of G and suppose that G contains an element x of order d. Then the subgroup G_d generated by x is of cardinality d, and all of its elements g satisfy $g^d = 1$. However, in the field K, the polynomial equation $X^d - 1 = 0$ has at most d solutions, which means that G_d has to be the set of these solutions. As it is cyclic of order d, it contains $\varphi(d)$ elements of order d which are the same elements as those of order d in G (any element of order d in G satisfies the equation $X^d - 1 = 0$, i.e., is in G_d). We have therefore shown that for any d that divides n, G has either 0 or $\varphi(d)$ elements of order d, i.e., at most $\varphi(d)$ elements of order d. From the lemma, we have that $n > \sum_{d|n, d\neq n} \varphi(d)$, and would thus have a contradiction if G had no elements of order n. This proves that G is cyclic.

□

Corollary 2.23 *If p is prime, the group $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic (and thus isomorphic to $\mathbf{Z}/(p-1)\mathbf{Z}$).*

Indeed, in this case $\mathbf{Z}/p\mathbf{Z}$ is a field (special case of proposition 2.19). Note that to find a generator of $(\mathbf{Z}/p\mathbf{Z})^*$ explicitly is algorithmically hard in general.

We now move on to the general setting.

Theorem 2.24 *Let p be prime ($p \neq 2$) and $\alpha \in \mathbf{N}^*$. Then the group $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ is cyclic (and thus isomorphic to the additive group $\mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$).*

We will see later that this result is false if $p = 2$ and $\alpha \geq 3$.

To prove the theorem, we begin by showing the existence of an element of order $p^{\alpha-1}$ in $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ with the help of the following lemma.

Lemma 2.25 *Let p be prime ($\neq 2$) and $k \in \mathbf{N}^*$. Then*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

with λ an integer not divisible by p.

Proof: We proceed by induction on k. For $k = 1$, we write

$$(1+p)^p = 1 + pC_p^1 + p^2C_p^2 + \ldots + p^p = 1 + p^2(1 + C_p^2 + \ldots + p^{p-2})$$

and use the fact that p divides C_p^k for $1 \leq k \leq p-1$ (note that for $p = 2$ this step does not work since p does not divide p^{p-2}), which implies that

$$1 + C_p^2 + \ldots + p^{p-2}$$

is not divisible by p.

Now suppose that the result is true for k. Thus,

$$(1+p)^{p^{k+1}} = (1+\lambda p^{k+1})^p = 1 + \lambda p^{k+2} + p^{k+2} \sum_{i=2}^{p} C_p^i \lambda^i p^{i(k+1)-(k+2)},$$

and since p divides $\sum_{i=2}^{p} C_p^i \lambda^i p^{i(k+1)-(k+2)}$ (it divides C_p^i for $2 \leq i \leq p-1$, and $p^{p(k+1)-(k+2)}$), we obtain that

$$\lambda' := \lambda + \sum_{i=2}^{p} C_p^i \lambda^i p^{i(k+1)-(k+2)}$$

is not divisible by p by the induction hypothesis. The lemma is therefore proved.

□

We also require a classical lemma on abelian groups:

Lemma 2.26 *Let G be an abelian group, given multiplicatively. Let $x \in G$ be an element of order a and $y \in G$ an element of order b. If a and b are coprime, then the order of xy is ab.*

Note that the result is false if we do not assume a and b are coprime (take $y = x^{-1}$), and also false in a non-abelian group if x and y do not commute (take a transposition and a 3-cycle in $\mathcal{S}_3$).

Proof of lemma 2.26: Let $n \in \mathbf{N}^*$ such that $(xy)^n = 1$. Then, $x^n = y^{-n}$, whereby $y^{-na} = 1$ and b divides na. As b is prime to a, we obtain that b divides n and also a divides n, from which ab divides n (also because $(a,b) = 1$). Since it is also true that $(xy)^{ab} = 1$, we see that the order of xy is indeed ab.

□

Proof of theorem 2.24: According to lemma 2.25, the element $s = \overline{1+p}$ is of order $p^{\alpha-1}$ in $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. We now look for an element of order $p-1$. We have an onto homomorphism $\pi : (\mathbf{Z}/p^\alpha\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ obtained by mapping $\bar{x}$ to the class of x modulo p (in effect, x is invertible modulo p^α if and only if it is invertible modulo p). Let u be a generator of $(\mathbf{Z}/p\mathbf{Z})^*$ (which is cyclic from corollary 2.23) and $v \in (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ such that $\pi(v) = u$. Let m be of order v, then $v^m = \bar{1}$ and therefore $u^m = \pi(v^m) = \bar{1}$ and $p-1$ (which is of order u) divides m. Setting $r = v^{m/(p-1)}$, we have that r is of order $p-1$ in $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. Now rs is of order $(p-1)p^{\alpha-1}$ in $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ by lemma 2.26.

□

The $p = 2$ case is special and comes with its own theorem:

Theorem 2.27 *For any integer $\alpha \geq 3$, the multiplicative group $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ is isomorphic to the additive group $\mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2^{\alpha-2}\mathbf{Z})$.*

Thus for $\alpha \geq 3$ the group $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ is not cyclic (the order of all elements divides $2^{\alpha-2}$). The $\alpha = 1$ and $\alpha = 2$ cases are trivial, $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ being respectively isomorphic to $\{0\}$ and $\mathbf{Z}/2\mathbf{Z}$.

Proof: It is easy to show by induction on $k \geq 1$ that we have : $5^{2^k} = 1 + \lambda 2^{k+2}$, where λ is some odd integer. As a result, the order of $\bar{5}$ in $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ is exactly $2^{\alpha-2}$; in other word, the subgroup N generated by $\bar{5}$ is of cardinality $2^{\alpha-2}$. Its intersection with the subgroup $C = \{\pm\bar{1}\}$ is $\bar{1}$, since any power of 5 (unlike for -1) is congruent with 1 modulo 4. Thus, $(n, c) \mapsto nc$ is a one-to-one homomorphism from $N \times C$ to $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$, and is therefore an isomorphism due to cardinality. We conclude by noting that N is isomorphic to the additive group $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ and $(\mathbf{Z}/4\mathbf{Z})^*$ to the additive group $\mathbf{Z}/2\mathbf{Z}$.

□

We conclude this section by stating the finite abelian group structure theorem, the proof of which will be given in the chapter on modules (an abelian group being nothing but a module over the ring $\mathbf{Z}$).

Theorem 2.28 *Let A be a finitely generated abelian group. Then there exists an integer $r \in \mathbf{N}$ and integers $d_1, \ldots, d_m$ with values ≥ 2 satisfying :*

a) The group A is isomorphic to the direct product $\mathbf{Z}^r \times \mathbf{Z}/d_1 \times \ldots \times \mathbf{Z}/d_m$.

b) We have $d_1|d_2|\ldots|d_m$.

Furthermore, this decomposition is unique.

3. Further details related to normal subgroups

3.1. Exact sequences

We start with the very useful notion of an *exact sequence*, which can also be extended to vector spaces (and, as we will see later, to modules).

Definition 3.1 We say that a (finite or infinite) sequence

$$\ldots \to G_i \stackrel{f_i}{\to} G_{i+1} \stackrel{f_{i+1}}{\to} G_{i+2} \to \ldots$$

is *exact* (here the G_i are groups and the f_i homomorphisms) if for any i, we have $\operatorname{Im} f_i = \ker f_{i+1}$. In particular,

$$1 \to N \overset{i}{\to} G \overset{p}{\to} H \to 1$$

is an exact sequence (said to be *short*) if and only if the following three properties hold : i is one-to-one, p is onto, and $\operatorname{Im} i = \ker p$. In this case, we have $G/N \simeq H$ (by matching N with $i(N)$) via the factorization theorem, and we say that G is an *extension* of H by N. [12]

Remark 3.2 a) Just as subgroups and quotients should not be confused, neither should "larger groups" (with respect to inclusion) and extensions be.

b) When all of the groups are abelian and given additively, we often write 0 instead of 1 in short exact sequences.

Example 3.3 a) If K is a field, then the sequence

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \overset{\det}{\to} K^* \to 1$$

is exact.

b) The sequences

$$1 \to SO_n(\mathbf{R}) \to O_n(\mathbf{R}) \overset{\det}{\to} \{\pm 1\} \to 1$$

and

$$1 \to SU_n(\mathbf{C}) \to U_n(\mathbf{C}) \overset{\det}{\to} S^1 \to 1$$

are exact, where S^1 designates the multiplicative group of complex numbers of modulus 1. Here $O_n(\mathbf{R})$ (resp. $U_n(\mathbf{C})$) is the orthogonal group (resp. unitary group) made up of real (resp. complex) matrices A of size (n, n) for which $A^*A = I_n$.

c) If $n \geq 2$, the sequence

$$1 \to \mathcal{A}_n \to \mathcal{S}_n \overset{\varepsilon}{\to} \{\pm 1\} \to 1$$

is exact.

d) Let G be a group with center Z. The group $(\operatorname{Int} G, \circ)$ of interior automorphisms of G is isomorphic to G/Z via the exact sequence

$$1 \to Z \to G \overset{\mathrm{int}}{\to} \mathrm{Int}G \to 1.$$

[12] Certain authors, e.g., D. Perrin, instead call this an extension of N by H.

e) The group $\mathbf{Z}/4$ can be seen as an extension of $\mathbf{Z}/2$ by $\mathbf{Z}/2$, via the exact sequence

$$0 \to \mathbf{Z}/2 \to \mathbf{Z}/4 \to \mathbf{Z}/2 \to 0, \tag{1}$$

where the arrow $\mathbf{Z}/4 \to \mathbf{Z}/2$ maps each $\bar{x} \in \mathbf{Z}/4$ to the class of x in $\mathbf{Z}/2$, and the arrow $\mathbf{Z}/2 \to \mathbf{Z}/4$ maps each $\bar{y} \in \mathbf{Z}/2$ to the class $2y$ in $\mathbf{Z}/4$. Note that $\mathbf{Z}/4$ is nevertheless not isomorphic to the product of $\mathbf{Z}/2$ with itself.

3.2. Semidirect product of groups

Be careful with this notion as it tends to be the source of many errors, notably at the oral examination for the *agrégation*.

Recall that when G_1 and G_2 are groups, we have the direct product $G_1 \times G_2$, which corresponds to defining the law $(g_1, g_2)(h_1, h_2) = (g_1 g_2, h_1 h_2)$ on the product set.

The semidirect product generalizes this idea. Let N and H be groups and $\varphi : H \to \mathtt{Aut}N$ a group homomorphism, one that in particular defines an action $h.n := \varphi(h)(n)$ of N on H (but here we ask also that the action is by automorphisms, i.e., the image of φ has to be contained in $\mathtt{Aut}N$, and not only in $\mathcal{S}(N)$).

Theorem 3.4 *Let us define a group law on the product set $N \times H$ as follows:*

$$(n, h).(n', h') := (n(h.n'), hh').$$

This group is called the semidirect product of N and H with respect to the action φ; this is denoted $N \rtimes_\varphi H$ (or simply $N \rtimes H$ if the action φ is implied).

Proof: Clearly, $(1, 1)$ is the identity element of the law as defined (we already use here that $h.1 = 1$, which comes from the fact that the action takes values in $\mathtt{Aut}N$). Also, (n, h) has the inverse $(h^{-1}.n^{-1}, h^{-1})$ (to see this is also a left inverse, we use $h^{-1}.(n^{-1}n) = (h^{-1}.n^{-1})(h^{-1}.n)$). All that is left is to show associativity.

We have

$$[(n_1, h_1)(n_2, h_2)](n_3, h_3) = (n_1(h_1.n_2), h_1 h_2)(n_3, h_3) = (n_1(h_1.n_2)[(h_1 h_2).n_3], h_1 h_2 h_3)$$

and

$$(n_1, h_1)[(n_2, h_2)](n_3, h_3)] = (n_1, h_1)(n_2(h_2.n_3), h_2 h_3) = (n_1[h_1.(n_2(h_2.n_3))], h_1 h_2 h_3).$$

However, $(h_1.n_2)[(h_1h_2).n_3] = [h_1.(n_2(h_2.n_3))]$ due to the axioms of group action and the fact that $n \mapsto h_1.n$ is an automorphism of N. The result follows.

□

Remark 3.5 a) Speaking of the semidirect product of N and H only makes sense if we provide the action; several actions may exist and thus several semidirect products. Also always keep in mind that N and H do not play the same role in the definition and are not interchangeable.

b) The trivial action corresponds to the direct product.

Proposition 3.6 *With the above notation, let $G = N \rtimes H$. Then :*

a) We have an exact sequence

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

with $i(n) = (n, 1)$ and $p(n, h) = h$. In particular N identifies to a normal subgroup (still denoted N) [13] in G.

b) The exact sequence is split, i.e., there exists a homomorphism $s : H \to G$ ("splitting") satisfying $p \circ s = \mathrm{Id}_H$. Thus H identifies to a subgroup (still denoted H) of G.

c) In G, we have $N \cap H = \{1\}$ and $NH = G$, where NH is by definition the set of nh with $n \in N$ and $h \in H$. Further, the action of H on N is given by $h.n = hnh^{-1}$, where the right product takes place in G.

Proof: a) i and p are homomorphisms via

$$(n, 1)(n', 1) = (n(1.n'), 1) = (nn', 1)$$

and

$$(n, h)(n', h') = (n(h.n'), hh').$$

It is immediately obvious that the sequence is exact.

b) It suffices to set $s(h) = (1, h)$.

c) From (a), $N \cap H$ is the set of (n, h) with $n = h = 1$, and is thus simply the identity element of G. If $g = (n, h)$ is an element of G, we have $g = (n, 1).(1, h)$, and thus $G = NH$. Finally, in G we have:

$$hnh^{-1} = (1, h)(n, 1)(1, h^{-1}) = (h.n, h)(1, h^{-1}) = (h.n, 1) = h.n.$$

[13] the symbol $\rtimes$ resembles $\lhd$ and helps us to remember the "direction" in which the semidirect product is taken.

□

Via the previous proposition, we can now write the elements of $N \rtimes H$ uniquely in the form nh $(n \in N, h \in H)$ with the commutativity rule given by $hn = (h.n)h$.

Remark 3.7 Suppose $G := N \rtimes_\varphi H$. If $H \lhd G$, we have $n^{-1}(h.n)h \in H$ (for all $n \in N$, $h \in H$) because $n^{-1}(h.n)h = n^{-1}hn \in H$. This implies that $n^{-1}(h.n) \in H$ and since $N \cap H = \{1\}$, we have that $n^{-1}(h.n) = 1$, i.e., the action is trivial. The semidirect product is abelian if and only if this condition holds and N and H are both abelian.

There is a kind of inverse version of the previous proposition to help know when a group can be broken down into a semidirect product.

Proposition 3.8 *a) ("Internal" form) Let G be a group containing subgroups N and H, where*

i) $N \lhd G$,

ii) $N \cap H = \{1\}$,

iii) $G = NH$.

Then $G \simeq N \rtimes H$ for the action $h.n = hnh^{-1}$.

b) ("External" form) Let

$$1 \to N \to G \to H \to 1$$

be an exact sequence that admits a splitting $s : H \to G$. Then $G \simeq N \rtimes H$ for the action $h.n = s(h)ns(h)^{-1}$.

Proof: a) Let φ be the action of H on N defined by $\varphi(h)(n) = hnh^{-1}$. Then the function $\Phi : N \rtimes_\varphi H \to G$ which associates with (n, h) the product nh (in G) is a homomorphism since $\Phi((n, h)(n', h')) = \Phi(n(hn'h^{-1}), hh') = nhn'h'$. Φ is one-to-one from (ii) and onto from (iii).

b) Set $H_1 = s(H)$. As s is one-to-one seeing as $p \circ s = \mathrm{id}_H$, H_1 is a subgroup of G isomorphic to H and from (a) it suffices to show that : $N \cap H_1 = \{1\}$ and $NH_1 = G$ (we have identified N with its image in G). If $h_1 \in N \cap H_1$, then $p(h_1) = 1$ but $h_1 = s(h)$ with $h \in H$, from which $1 = p(s(h)) = h$ and $h_1 = 1$. If now $g \in G$, then g and $s(p(g))$ have the same image under p, so they differ by one element from the kernel N of p, i.e., $g = nh_1$ with $h_1 := s(p(g))$, and $g \in NH_1$.

□

It is in general the second criterion which is the most useful for obtaining semi-direct product decompositions, but we will keep clearly in mind the way

to determine the operation of H on N according to the exact sequence and the splitting.

Remarque 3.9 We will see in the exercice sessions two sufficient conditions to obtain isomorphic semi-direct products for various actions :

a) Let N and H be groups, and φ and ψ homomorphisms $H \to \mathtt{Aut}N$. If there exists $u \in \mathtt{Aut}N$ such that $\psi(h) = u \circ \varphi(h) \circ u^{-1}$ ("conjugate actions"), we have that $N \rtimes_\varphi H \simeq N \rtimes_\psi H$.

b) Let N and H be groups, and φ and ψ homomorphisms $H \to \mathtt{Aut}N$. If there exists $\alpha \in \mathtt{Aut}H$ such that $\varphi = \psi \circ \alpha$, then $N \rtimes_\varphi H \simeq N \rtimes_\psi H$.

Example 3.10 a) For $n \geq 2$, the exact sequence

$$1 \to \mathcal{A}_n \to \mathcal{S}_n \xrightarrow{\varepsilon} \mathbf{Z}/2\mathbf{Z} \to 1$$

admits the splitting s which maps $\bar{0}$ onto Id and $\bar{1}$ onto an (arbitrary) transposition τ. We can then deduce the decomposition: $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbf{Z}/2\mathbf{Z}$.

b) Let K be a field and $n \in \mathbf{N}^*$. The exact sequence

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^* \to 1$$

is split (map $\lambda \in K^*$ onto the matrix $\mathrm{Diag}(\lambda, 1, \ldots, 1)$). Thus, $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^*$.

c) The group $\mathbf{Z}/4\mathbf{Z}$ is *not* a semi-direct product of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$. In effect, it is a *direct* product since $\mathbf{Z}/4\mathbf{Z}$ is abelian. However, $\mathbf{Z}/4\mathbf{Z}$ is not isomorphic to the direct product $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (the former has elements of order 4 but not the latter). In particular, the exact sequence (1) in example 3.3 is not split.[14]

d) Let $n \geq 3$, and note D_n the *dihedral group* (consisting of isometries of a regular n-sided polygon). This contains the n rotations with center O (the center of the polygon) and angle $2k\pi/n$ ($0 \leq k \leq n-1$) and the n reflections with respect to lines passing by O and the vertices (if n is odd) or the midpoints of the edges (if n is even). We have an exact sequence

$$1 \to \mathbf{Z}/n\mathbf{Z} \to D_n \to \mathbf{Z}/2\mathbf{Z} \to 1$$

by taking the determinant of a given isometry, with values in $\{\pm 1\}$. It is split (we map the nontrivial element ε from $\mathbf{Z}/2\mathbf{Z}$ to a reflection), leading to the decomposition $D_n \simeq \mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$. Note that the corresponding action from $\mathbf{Z}/2\mathbf{Z}$ to $\mathbf{Z}/n\mathbf{Z}$ consists in setting $\varepsilon.x = -x$ for $x \in \mathbf{Z}/n\mathbf{Z}$.

[14] We thus see that even in very simple cases, we cannot always "reconstitute" a group from its subgroups. In particular, knowledge of simple finite groups is absolutely not sufficient in order to know all finite groups, contrary to fairly widespread popular belief (especially among students taking the *agrégation* exam!).

A study of the group of automorphisms of $\mathbf{Z}/n\mathbf{Z}$ makes it possible to construct nontrivial semi-direct products. Here is a simple application of this idea :

Theorem 3.11 *Let p and q be primes with $p < q$. Then :*

- *If p does not divide $q-1$, any group of order pq is cyclic.*
- *If p divides $q-1$, there are two (isomorphic) groups of order pq : the cyclic group, and a semi-direct product $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$ (which is non-abelian).*

For example, the only group of order 15 is $\mathbf{Z}/15\mathbf{Z}$, and for $q \geq 3$, the two groups of order $2q$ are the cyclic group and the dihedral group D_q.

Proof: Let G be of order pq. Then G has a q-Sylow Q. According to Sylow's second theorem, the number of q-Sylows is congruent to 1 mod q, and divides p, so is therefore 1 since $p < q$. Hence Q is normal in G. We thus obtain an exact sequence

$$1 \to Q \to G \xrightarrow{f} G/Q \to 1.$$

We show now that this sequence is split: the group G contains a p-Sylow P, the restriction of f to P is thus one-to-one since the cardinality of its kernel $P \cap Q$ must divide p and q. Hence f induces a bijection from P to G/Q, and the inverse bijection provides the required splitting. Hence G is a semi-direct product $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$, associated with a homomorphism $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathtt{Aut}(\mathbf{Z}/q\mathbf{Z}) \simeq \mathbf{Z}/(q-1)\mathbf{Z}$.

If p does not divide $q-1$, the cardinality of the image of φ divides p and $q-1$, and is thus 1, i.e., φ is constant and the product is direct. As p and q are prime, G is isomorphic to $\mathbf{Z}/pq\mathbf{Z}$ via the Chinese remainder theorem.

If p does not divide $q-1$, we have a nontrivial homomorphism φ by mapping $\bar{1}$ onto the class of $(q-1)/p$, and thus a noncommutative semi-direct product. The fact that up to isomorphism this is the only one follows easily from remark 3.9 (b).

□

3.3. Simple groups, the alternating group example

Recall that a group is *simple* if its only nontrivial normal subgroups are itself and $\{1\}$. For example, the simple abelian groups are the $\mathbf{Z}/p\mathbf{Z}$ where p is prime. It is not necessarily easy to find other examples of simple groups. The goal of this section is to prove the following theorem.

Theorem 3.12 *For $n \geq 5$, the alternating group $\mathcal{A}_n$ is simple.*

Note that the result is also (trivially) true for $n = 2$ and $n = 3$, but not for $n = 4$, since the group made up of double transpositions in $\mathcal{A}_4$ is a nontrivial normal subgroup.

Before moving to the proof, we first look at a few corollaries of this result.

Corollary 3.13 *For $n \geq 5$, we have $D(\mathcal{A}_n) = \mathcal{A}_n$ and $D(\mathcal{S}_n) = \mathcal{A}_n$.*

Note that the second assertion is true for all $n \geq 2$ (only the $n = 4$ case needs to be proved separately, see the tutorials).

Proof: We have $D(\mathcal{A}_n) \subset \mathcal{A}_n$ given that any commutator has a signature of 1, but $D(\mathcal{A}_n)$ is normal in $\mathcal{A}_n$ and nontrivial given that for $n \geq 4$, $\mathcal{A}_n$ is non-abelian (two 3-cycles whose supports have one or two shared elements do not commute). Hence $D(\mathcal{A}_n) = \mathcal{A}_n$ as $\mathcal{A}_n$ is simple. Similarly, $D(\mathcal{S}_n)$ is a nontrivial subgroup of $\mathcal{A}_n$, normal in $\mathcal{A}_n$ (it is already normal in $\mathcal{S}_n$), so $D(\mathcal{S}_n) = \mathcal{A}_n$ from the theorem.

□

Corollary 3.14 *If $n \geq 5$, $\mathcal{S}_n$ has three normal subgroups : $\{\mathrm{Id}\}$, $\mathcal{A}_n$, and $\mathcal{S}_n$.*

Proof: Let H be a normal subgroup of $\mathcal{S}_n$. Then, $H \cap \mathcal{A}_n$ is normal in $\mathcal{A}_n$, so by the theorem, $H \cap \mathcal{A}_n$ is equal to $\mathcal{A}_n$ or reduced to $\{\mathrm{Id}\}$. In the former case, $H \supset \mathcal{A}_n$, thus $H = \mathcal{A}_n$ or $H = \mathcal{S}_n$ since $\mathcal{A}_n$ has an index of 2 in $\mathcal{S}_n$. Suppose therefore that $H \cap \mathcal{A}_n = \{\mathrm{Id}\}$ and let us show that H is the trivial group. If τ and σ are (different) nontrivial elements in H, then $\tau\sigma$ has a signature of $(-1)(-1) = 1$, so $\tau = \sigma^{-1}$. From this, $H = \{\mathrm{Id}, \sigma, \sigma^{-1}\}$, but then H is an onto map to $\{\pm 1\}$ by the signature, which is impossible as it is of cardinality 3, and 2 does not divide 3. This means that H has to be of cardinality 1 ou 2. However, a subgroup of cardinality 2 of $\mathcal{S}_n$ is of the form $\{\mathrm{Id}, \tau\}$ where τ is a product of transpositions whose supports are disjoint, so such a subgroup cannot be normal if $n \geq 3$, which can be seen using calculations similar to those in example 1.19 (d).

□

Corollary 3.15 *Let H be a subgroup with index n of $\mathcal{S}_n$ for $n \geq 2$. Then, $H \simeq \mathcal{S}_{n-1}$.*

Proof: The $n = 2$ and $n = 3$ cases are trivial. For $n = 4$, H is of cardinality 6, but cannot be cyclic (there are no elements of order 6 in $\mathcal{S}_4$, seeing that the order of an element is the least common multiple of the length of the cycles in its decomposition) so is isomorphic to the dihedral group D_3, i.e., to $\mathcal{S}_3$. Suppose therefore that $n \geq 5$. Then, $\mathcal{S}_n$ acts by translation on the set $E := \mathcal{S}_n/H$ of left cosets, from which comes a homomorphism $\varphi : \mathcal{S}_n \to \mathcal{S}(E)$. The kernel is a normal subgroup of $\mathcal{S}_n$, and cannot contain $\mathcal{A}_n$ since this kernel is inside H (the stabilizer of the identity element's class is H), which is of cardinality $(n-1)! < \frac{n!}{2}$. From the previous corollary, the kernel is thus trivial. Hence, φ is one-to-one, and since E is of cardinality n, it is an isomorphism. Now define $U := \varphi(H)$. As we have seen, the subgroup $U \subset \mathcal{S}(E)$ is the stabilizer of the element H in E. As E is of cardinality n, we get that U (which is isomorphic to H) is isomorphic to the stabilizer of a point in $\mathcal{S}_n$, i.e., to $\mathcal{S}_{n-1}$.

□

Remark 3.16 This corollary does not imply that H is the stabilizer of a point for the natural action of $\mathcal{S}_n$ on $\{1, \ldots, n\}$. This is however true if $n \neq 6$, and is linked to the fact that for $n \neq 6$, the only automorphisms of $\mathcal{S}_n$ are interior ones (see tutorials).

Proof that $\mathcal{A}_n$ is simple for $n \geq 5$. The proof requires two fairly simple lemmas :

Lemma 3.17 *For $n \geq 3$, the 3-cycles generate $\mathcal{A}_n$.*

Proof: Since $\mathcal{S}_n$ is generated by the transpositions, $\mathcal{A}_n$ is generated by the products of transpositions. Then, if a, b, c, d are four distinct elements in $[1, n]$, we have $(a, b)(b, c) = (a, b, c)$, $(a, b)(a, c) = (a, c, b)$, and $(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, c, b)(a, c, d)$.

□

Lemma 3.18 *For $n \geq 5$, the 3-cycles are conjugate in $\mathcal{A}_n$.*

Proof: Let $\tau = (a_1, a_2, a_3)$ and $\tau' = (b_1, b_2, b_3)$ be 3-cycles. Then, there exists $\sigma \in \mathcal{S}_n$ such that $\sigma(a_i) = b_i$ for $i = 1, 2, 3$, from which $\sigma\tau\sigma^{-1} = \tau'$. If $\varepsilon(\sigma) = 1$, we are done. Otherwise, replace σ by $\sigma' = \sigma(c, d)$, where c and d are two distinct elements in $[1, n]$ and also distinct in a_1, a_2, a_3 (here, the hypothesis $n \geq 5$ is used).

□

As a result of these lemmas, any normal subgroup of $\mathcal{A}_n$ containing a 3-cycle is equal to $\mathcal{A}_n$ if $n \geq 5$.

We now prove the result for $n = 5$:

Proposition 3.19 *The group $\mathcal{A}_5$ is simple.*

Proof: The cardinality of $\mathcal{A}_5$ is 60. We begin by sorting its elements by their order, using their decompositions into cycles.

The elements of order 2 are the products of transpositions with disjoint supports; there are $5 \times 3 = 15$ of these (5 choices for the fixed point, and 3 double transpositions in $\mathcal{S}_4$).

The elements of order 3 are the 3-cycles, of which there are $C_5^3 \times 2 = 20$ (C_5^3 choices for the permuted elements, and two 3-cycles in $\mathcal{S}_3$).

There is no element of order 4 (the 4-cycles have a signature of -1).

The elements of order 5 are the 5-cycles, of which there are $4! = 24$, since a 5-cycle c corresponds to providing $c(1)$ (4 choices), then $c^2(1)$ (3 choices), etc.

Now, suppose H is a normal subgroup of $\mathcal{A}_5$. We show that if H contains an element of order ω, with $\omega \in \{2, 3, 5\}$, then it contains all of the elements of order ω. If $\omega = 3$, this is a result of the first lemma. If $\omega = 2$, it suffices to see that the elements of order 2 are conjugate in $\mathcal{A}_5$; however, if $\tau = (a_1, a_2)(a_3, a_4)(a_5)$ and $\tau' = (b_1, b_2)(b_3, b_4)(b_5)$ are two such elements, there exists an element σ in $\mathcal{S}_5$ such that $\sigma(a_i) = b_i$ for $i = 1, \ldots, 5$, and thus $\sigma\tau\sigma^{-1} = \tau'$. If σ has a signature of -1, we replace it by $\sigma(a_2, a_1)$. Finally, while the 5-cycles are not all conjugate in $\mathcal{A}_5$[15], the subgroups of order 5 are, since these are the 5-Sylows of $\mathcal{A}_5$; hence if H contains an element of order 5, it contains the subgroup generated by it, thus all of the subgroups of order 5, and therefore all of the elements of order 5.

Now suppose that $H \neq \{\mathrm{Id}\}$. Then there can exist no $\omega \in \{2, 3, 5\}$ such that all nontrivial elements in H are of order ω, because otherwise, after what we have just seen, H would be of cardinality $15 + 1$, $20 + 1$, or $24 + 1$, and none of these numbers divide 60. There must therefore be at least two numbers ω and ω' out of $2, 3, 5$ for which H contains all of the elements of order ω and ω', but if so, the cardinality of H would be greater than $60/2$, and $H = \mathcal{A}_5$ since its cardinality must divide 60.

□

In fact, $\mathcal{A}_5$ is the smallest simple group apart from the $\mathbf{Z}/p\mathbf{Z}$ with prime p (see tutorials).

[15] In fact, if c and c' are 5-cycles, c is conjugate to either c' or c'^2, which is all that is required for the current argument.

Proof of the theorem in the general case. Let $E = [1, n]$ and suppose H is a subgroup of $\mathcal{A}_n$ that is not simply the identity element. Choose a nontrivial σ in H. We intend to manoeuvre ourselves to the $n = 5$ case by constructing an element of H which acts on a subset of cardinality of at most 5 in E. For this, we are not going to consider a conjugate of σ (which would have the same number of fixed points as σ), but a commutator $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$ (which has a chance of having more). We choose τ in the following way : let a be in E such that $b := \sigma(a)$ is distinct from a, then c in E distinct from a, b, and $\sigma(b)$. We then set $\tau = (a, c, b)$, which means that $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$ is indeed in H. Then, $\tau^{-1} = (a, b, c)$, from which $\rho = (a, c, b)(\sigma\tau^{-1}\sigma^{-1}) = (a, c, b)(\sigma.a, \sigma.b, \sigma.c)$. As $\sigma.a = b$, we see that there exists a subset F of E which has at most 5 elements (and we can take one whose cardinality is exactly 5) such that ρ acts trivially outside F, and F contains $\{a, b, c, \sigma(b), \sigma(c)\}$.

This gives us a one-to-one homomorphism i from $\mathcal{A}(F)$ to $\mathcal{A}_n$ by extending a permutation of F to the identity outside F. Now, set $H_0 = i^{-1}(H)$, which is a normal subgroup of $\mathcal{A}(F) \simeq \mathcal{A}_5$. However, H_0 is not trivial because it contains the restriction of ρ to F, and we have $\rho(b) = \tau\sigma(b) \neq b$ (seeing as $\sigma(b) \neq c = \tau^{-1}(b)$). Thus, $H_0 = \mathcal{A}(F)$ thanks to the $n = 5$ case. In particular, H_0 contains a 3-cycle, so H does too, and therefore $H = \mathcal{A}_n$ via the two lemmas.

□

3.4. Solvable and nilpotent groups

Here we stick to a few definitions and initial properties of these. A more in-depth treatment can be found in Hall's text [1].

Definition 3.20 Let G be a group[16]. We say that G is *solvable* if there exists a finite sequence

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

whereby for any $i \in [1, n]$, $G_{i-1} \lhd G_i$ and G_i/G_{i-1} is abelian.

The following characterization of solvable groups is useful:

Proposition 3.21 *Let G be a group, and set $D^0(G) = G$, $D^1(G) = D(G)$, and $D^i(G) = D(D^{i-1}(G))$ for all $i \geq 2$. Then G is solvable if and only if there exists an integer n such that $D^n(G) = \{1\}$.*

[16]This notion is of most interest for finite groups, but is not necessarily limited to them.

Proof: If there exists an n such that $D^n(G) = \{1\}$, then each quotient $D^i(G)/D^{i-1}(G)$ is an abelian group by the definition of commutator subgroups, so G is solvable via the sequence of $D^i(G)$. Note that each $D^i(G)$ is normal in G itself since the derived subgroup of a group H is characteristic in H, and this property is transitive.

In the reverse direction, if G is solvable, let $(G_i)_{1 \leq i \leq n}$ be a sequence like in definition 3.20. Then, G/G_{n-1} is abelian, so $G_{n-1} \supset D(G)$. By induction on i, we have $G_{n-i} \supset D^i(G)$ (if $G_{n-i+1} \supset D^{i-1}(G)$, and thus since G_{n-i+1}/G_{n-i} is abelian, we have $G_{n-i} \supset D(G_{n-i+1}) \supset D(D^{i-1}(G)) = D^i(G)$). For $i = n$, this gives $D^n(G) = \{1\}$.

□

Remark 3.22 a) Proposition 3.21 says that we can also require that each G_i be normal in G (using the sequence of commutator subgroups $D^i(G)$). Thus, G solvable means that it can be deduced, starting from $\{1\}$, using a finite sequence of *extensions with abelian kernels* :

$$1 \to G_i/G_{i-1} \to G/G_{i-1} \to G/G_i \to 1.$$

b) If G is finite and we do not impose that $G_i \lhd G$, we can instead require that G_i/G_{i-1} be cyclic with prime order instead of abelian; in effect, any finite abelian group H has a sequence $H \supset \ldots \supset \{1\}$ where all of the H_i/H_{i-1} are simple (and thus cyclic with prime order since they are abelian), which can be shown by induction on $\#H$. On the other hand, requiring that G_i/G_{i-1} be cyclic and $G_i \lhd G$ for all i is a stronger condition (the groups here are called *supersolvable*).

c) The term *solvable* comes from Galois theory. If P is an irreducible polynomial with coefficients in $\mathbf{Q}$, and $K \subset \mathbf{C}$ its *splitting field* (the smallest field containing all of its roots), we define the *Galois group* G of P as the group of automorphisms of the field K. Galois theory states that the equation $P(x) = 0$ is solvable by radicals if and only if G is solvable. The fact that $\mathcal{S}_n$ is not solvable for $n \geq 5$ implies that there is no solution in radicals to general polynomial equations of degree 5. We will see this in more detail in the chapter on Galois theory.

A concept even stronger than solvable (even more so than supersolvable for finite groups) is that of *nilpotent* groups :

Definition 3.23 We say that a group G is *nilpotent* if there exists a finite sequence

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

such that for any $i \in [1, n]$: $G_i \lhd G$ and the extension

$$1 \to G_i/G_{i-1} \to G/G_{i-1} \to G/G_i \to 1$$

is *central*, i.e., G_i/G_{i-1} is in the center of G/G_{i-1}.

This means that G can be deduced starting from $\{1\}$ using a finite sequence of central extensions.

Example 3.24 a) Abelian groups are nilpotent.

b) Any p-group G is nilpotent: this can be seen immediately using induction on its cardinality, given that its center is nontrivial if G is nontrivial, and the quotient of G by its center remains a p-group.

c) $\mathcal{S}_n$ and $\mathcal{A}_n$ are not solvable for $n \geq 5$. This is a result of $D(\mathcal{S}_n) = D(\mathcal{A}_n) = \mathcal{A}_n$, and proposition 3.21.

d) $\mathcal{S}_4$ is solvable via the sequence

$$\mathcal{S}_4 \supset \mathcal{A}_4 \supset V_4 \supset \{1\},$$

where V_4 is the subgroup made up of the identity and the double transpositions, but cannot be nilpotent since its center is trivial. The same conclusions hold for $\mathcal{A}_4$ and $\mathcal{S}_3$.

e) $\mathcal{S}_3$ is supersolvable but not $\mathcal{A}_4$.

f) A subgroup or quotient of a solvable group is solvable, as is the extension of a solvable group by a solvable group.

References

[1] M. Hall Jr : *The theory of groups*, The Macmillan Co., New York, N.Y. 1959.

[2] D. Perrin : *Cours d'algèbre*, Ellipses 1996.