1. Group Theory I

Section 2.2
We list some consequences of Lagrange's Theorem for exponents and orders of elements which will be used later, especially in 2.6.

Definition 1.1. *Let G be an arbitrary group and g an element of G. A natural number m is called* **exponent** *of g if g^m equals the unit element e of G.*

Examples If G is the Klein Four Group then 2 is an exponent of every $g \in G$. If G is finite then $|G|$ is an exponent for every $g \in G$. For $G = (\mathbb{Z}, +)$ the non-zero elements of G have no exponents whereas $0 \in G$ has every natural number as exponent. For $G = \mathbb{Q}^\times := (\mathbb{Q} \setminus \{0\}, \times)$ the element -1 has exponent 2 and the elements g with absolute value greater than 1 (similarly less than 1) have no exponents.

If an element $g \in G$ has an exponent m then it is quite natural to ask for the minimal exponent of g. As we saw in the previous examples the elements g of the Klein Four Group have minimal exponents either 1 ($g = e$) or 2, whereas the elements g of the cyclic group of order 4 can have minimal exponents 1,2,4. We note that the set of exponents of an element g is a subset of $\mathbb{N}$ and therefore contains a (unique) minimal element if it is not empty.

Definition 1.2. *Let G be an arbitrary group and g an element of G. If g has exponents $m \in \mathbb{N}$ then there exists a smallest exponent, the so-called* **order** *$ord(g)$ of g. In that case we say that g is of finite order (otherwise infinite).*

Remarks As a consequence of Lagrange's Theorem the order of an element g of a group G divides the group order $|G|$ in case G is finite. We observe that $\mathrm{ord}(e) = 1$.

It will turn out useful to establish a few properties of the order function for group elements, especially when discussing finite abelian groups.

Lemma 1.3. *Let g be an element of a group G of finite order $m = ord(g)$. Then we have*

$$ord(g^k) = ord(g)/gcd(k, m)$$

for every $k \in \mathbb{Z}$.

Proof We set $c := \gcd(k, m)$ and need to show that $d := m/c$ is the smallest exponent for m^k. Clearly, d is an exponent for m^k because of $(g^k)^d = g^{kd} = g^{mk/c} = (g^m)^{k/c} = e^{k/c} = e$. On the other hand, let f be any exponent for g^k. Because of $e = (g^k)^f = g^{kf}$ the element kf must be a multiple of m, say $kf = lm$ for an appropriate $l \in \mathbb{Z}$. This induces $\frac{k}{c}f = l\frac{m}{c}$ and $\frac{k}{c}$, $\frac{m}{c}$ being coprime we obtain indeed that $\frac{m}{c}$ divides f.

□

We note that we did not impose any conditions on the group G in the previous lemma. If we want to establish a relation between the orders of two group elements and the order of their product then we need to assume that these elements commute. The latter will become clear from the proof and the remarks thereafter.

Lemma 1.4. *Let g, h be commuting elements of a group G with coprime orders $m = ord(g)$ and $n = ord(h)$. Then the element $gh = hg$ has order mn.*

Proof Because of $(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = e$ the product mn is an exponent of gh. On the other hand, if f is any exponent of gh we put $c = \gcd(f, m)$, $d := \gcd(f, n)$ and get $e = ((gh)^f)^{m/c} = g^{m(f/c)}h^{fm/c} = h^{fm/c}$, respectively, $e = ((gh)^f)^{n/c} = g^{fn/c}h^{n(f/c)} = g^{fn/c}$. From the first equation we conclude that n divides $f(m/c)$ and since n and m were coprime this yields $n \mid f$. The second equation yields $m \mid f$ analogously and again, n and m being coprime we obtain that mn divides f. Hence, mn is indeed a minimal exponent for gh.

□

If the elements g, h do not commute then the order of their product cannot be obtained so easily. We observe that in the symmetric group $\mathcal{S}_3$ the product of an element of order 3 and one of order 2 has order 2 again (see **??**). It can even happen that the product of two elements of finite order has an infinite order . To see this we consider $\mathbb{R}$ as affine line and let G be the group of bijective affine mappings from $\mathbb{R}$ onto itself. It contains the 2 reflections $g(x) = 2 - x$ and $h(x) = -x$ of order 2 each. Then $gh \neq hg$, $hg(x) = x + 2$ and $gh(x) = x - 2$ are both translations, hence their order is infinite.

Even the case in which g, h commute but their orders are not coprime is not immediately deducible from the preceding lemmata. We note that the likely assumption $\mathrm{ord}(gh) = \mathrm{lcm}(\mathrm{ord}(g), \mathrm{ord}(h))$ is terribly false as the example $h = g^{-1}$ demonstrates.

Lemma 1.5. *Let g, h be commuting elements of a group G with orders $m = ord(g)$ and $n = ord(h)$. The order of the element $gh = hg$ divides*

$d := lcm(m,n)$. There exist exponents u, v such that the element $g^u h^v$ has order d.

Proof As in the proof of the previous lemma one immediately sees that d is an exponent of gh. To show the last statement we consider the prime number decompositions of m, n, respectively. We recall that every natural number can be written as a formal infinite product over all prime numbers in which only finitely many exponents are non-zero. So we assume that

$$m \,=\, \prod_{p\in\mathbb{P}} p^{m_p} \;,\; n \,=\, \prod_{p\in\mathbb{P}} p^{n_p}$$

and set

$$u \,:=\, \prod_{\substack{p\in\mathbb{P}\\ m_p<n_p}} p^{m_p} \;,\; v \,:=\, \prod_{\substack{p\in\mathbb{P}\\ n_p\leq m_p}} p^{n_p} \;\;.$$

Then the orders

$$\mathrm{ord}(g^u) \,:=\, \prod_{\substack{p\in\mathbb{P}\\ m_p\geq n_p}} p^{m_p}$$

and

$$\mathrm{ord}(h^v) \,:=\, \prod_{\substack{p\in\mathbb{P}\\ m_p<n_p}} p^{n_p}$$

are mutually prime and the previous lemma yields

$$\mathrm{ord}(g^u h^v) \,:=\, \prod_{\substack{p\in\mathbb{P}\\ m_p\geq n_p}} p^{m_p} \prod_{\substack{p\in\mathbb{P}\\ m_p<n_p}} p^{n_p} \;=\; \mathrm{lcm}(m,n) \;\;.$$

□

Example Let g, h be commuting elements of a group G with $m := \mathrm{ord}(g) = 540$, $n := \mathrm{ord}(h) = 1008$, respectively. We easily calculate $m = 2^2 3^3 5$, $n = 2^4 3^2 7$, $u = 2^2$, $v = 3^2$, hence we get

$$\mathrm{ord}(g^4) = 135,\; \mathrm{ord}(h^9) = 112,\; \mathrm{ord}(g^4 h^9) = 15120 \;\;.$$

Section 2.6 Making use of the concept of direct products we present the structure theorem for finite abelian groups.

We conclude this first chapter on groups by showing that every finite abelian group is a direct product of cyclic subgroups. Our approach is theoretically oriented at this stage but it will turn out later (see chapter 6) that the ideas introduced here can easily be transformed into algorithms. There they will also be extended to finitely generated abelian groups.

Theorem 1.6. *Every finite abelian group G is a direct product of cyclic subgroups:*

$$G \;=\; \dot{\prod_{i=1}^{l}} G_i \;\;.$$

Additionally, we can postulate that the orders $n_i :=\mid G_i \mid$ have the divisibility properties $n_{i+1} \mid n_i \;\; (1 \leq i < l)$. (The vector $(n_1, ..., n_l)$ is an invariant of the group G; the n_i are said to be **elementary divisors** *of G.)*

Proof. The proof is by induction on the order n of G. For $n = 1, 2, 3$ the group G itself is cyclic. Therefore we immediately proceed to the induction step $n \longrightarrow n + 1$.

For $G = \langle a_1, ..., a_k \rangle$ the order of each element $g \in G$ is a divisor of $\mathrm{lcm}(\mathrm{ord}(a_1), ..., \mathrm{ord}(a_k)) =: n_1$.

Because of Lemma **??** the group G contains an element A_1 with $\mathrm{ord}(A_1) = n_1$.

We set $G_1 := \langle A_1 \rangle$ and $\tilde{G} := G/G_1$. The order of $\tilde{G}$ is smaller than the order of G.

Because of our induction assumption the group $\tilde{G}$ is a direct product of cyclic subgroups, say

$$\tilde{G} \;=\; \dot{\prod_{i=2}^{l}} \langle b_i G_1 \rangle \;\; (b_i \in G) \;\;,$$

and the orders $n_i =\mid \langle b_i G_1 \rangle \mid$ satisfy $n_{i+1} \mid n_i \;\; (2 \leq i < l)$. (From this it is clear that $A_1, b_2, ..., b_l$ generate G, but the product of the corresponding cyclic subgroups is in general not direct. We therefore need to change the b_i adequately.)

Because of $n_i =\mid \langle b_i G_1 \rangle \mid$ the exponent n_i is minimal with the property $b_i^{n_i} \in G_1$, and therefore n_i divides every exponent μ satisfying

$b_i^{\mu} \in G_1$. As a consequence we have $n_i \mid \mathrm{ord}(b_i)$. We also know that $n_1 = \mathrm{ord}(b_i)\lambda_i$ for a suitable integer λ_i.

Let us assume that

$$b_i^{n_i} \;=\; A_1^{m_i} \;\; (0 \leq m_i < n_1) \;\; . \tag{1}$$

We want to show that n_i divides m_i.

Because of Lemma **??** we get

$$\mathrm{ord}(A_1^{m_i}) \;=\; \frac{n_1}{\gcd(n_1, m_i)} \;\; . \tag{2}$$

Analogogously, we obtain

$$\mathrm{ord}(b_i^{n_i}) \;=\; \frac{\mathrm{ord}(b_i)}{\gcd(\mathrm{ord}(b_i), n_i)} \;=\; \frac{\mathrm{ord}(b_i)}{n_i} \;\; . \tag{3}$$

Since $\mathrm{ord}(b_i)$ divides n_1 the equations (**??**), (**??**), and (**??**) yield

$$\frac{n_1}{\gcd(n_1, m_i)}\lambda_i \;=\; \frac{n_1}{n_i}$$

for the integer λ_i with $n_1 = \mathrm{ord}(b_i)\lambda_i$.

From this we conclude

$$n_i\lambda_i \;=\; \gcd(n_1, m_i) \;\mid\; m_i \;\; ,$$

hence, there is an integer τ_i with $n_i\tau_i = m_i$.

We put $A_i := b_i A_1^{-\tau_i}$ and obtain $b_i G_1 = A_i G_1$ as well as $\mathrm{ord}(A_i) = n_i$.

We still need to show

$$G \;=\; \dot{\prod_{i=1}^{l}} \langle A_i \rangle \;\; .$$

Because of $G = \langle A_1, b_2, ..., b_l \rangle$ we immediately get $\langle A_1, A_2, ..., A_l \rangle = G$. We have already shown that the product is also direct if the presentations of elements of $x \in G$ as power products of $A_1, ..., A_l$ in the form

$$x \;=\; \prod_{i=1}^{l} A_i^{\mu_i} \;\; (0 \leq \mu_i < n_i)$$

are unique.

For this we assume that $x \in G$ has presentations

$$x \;=\; \prod_{i=1}^{l} A_i^{\mu_i} \;=\; \prod_{i=1}^{l} A_i^{\nu_i} \;\; (0 \leq \mu_i, \nu_i < n_i) \;\; .$$

This yields

$$A_1^{\mu_1-\nu_1} \;=\; \prod_{i=2}^{l} A_i^{\nu_i-\mu_i} \tag{4}$$

and therefore also

$$\begin{aligned} G_1 &= \left(\prod_{i=2}^{l} A_i^{\nu_i-\mu_i}\right) G_1 \\ &= \prod_{i=2}^{l} (A_i G_1)^{\nu_i-\mu_i} \\ &= \prod_{i=2}^{l} (b_i G_1)^{\nu_i-\mu_i} \quad . \end{aligned}$$

According to our induction assumption we get

$$\nu_i - \mu_i \;=\; 0 \;\; (2 \le i \le l) \;\; .$$

Inserting this into (**??**) we also find $\mu_1 - \nu_1 = 0$, hence $\mu_i = \nu_i$ for $1 \le i \le l$.

By our construction, the divisibility conditions for the n_i are satisfied, too.

□

Example Let $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ of order 360. The least common multiple of the orders of the 3 cyclic subgroups is 60. An element A_1 of G of order 60 is easily found, for example, we can choose $A_1 = (1 + 4\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 15\mathbb{Z})$. Then the order of $G/\langle A_1\rangle$ is 6, that factor group is therefore cyclic, a generator is $(4\mathbb{Z}, 1+6\mathbb{Z}, 1+15\mathbb{Z})\langle A_1\rangle$. We set $b_2 = (4\mathbb{Z}, 1 + 6\mathbb{Z}, 1 + 15\mathbb{Z})$ and obtain $b_2^6 = A_1^{12}$. This results in $A_2 = b_2 A_1^{-2}$ and $G = \langle A_1\rangle \times \langle A_2\rangle$.

Because of our considerations about the orders of products of elements, especially Lemma **??**, the proof of the preceding theorem can be employed for actually calculating the presentation of G as a direct product as in the previous example. However, we postpone that algorithmic treatment until chapter 6 since it is advisable to use the machinery of normal forms of integral matrices which will be developed there.