A.10 Some Group Theoretic Trivia

Here we collect some elementary results on finite groups. The exponent of a group G is the minimum positive integer e (or ∞) such that $x^e = \mathbf{1}$ for all $x \in G$. Denote the order of a group element x by $\operatorname{ord} x$ (positive integer or ∞).

Lemma 20 *Let G be a finite group with exponent e. Then $e \mid \#G$, and $e = t := \operatorname{lcm}(\{\operatorname{ord} x \mid x \in G\})$.*

Proof. By LAGRANGE's Theorem $\operatorname{ord} x \mid \#G$ for all $x \in G$, hence $e \mid \#G$. Moreover $x^e = \mathbf{1}$ by definition of e, hence $\operatorname{ord} x \mid e$ for all $x \in G$. Hence $t \mid e$. Sinc $x^t = \mathbf{1}$ for all x, even $t = e$. $\diamond$

Lemma 21 *Let G and H be groups, $g \in G$ with $\operatorname{ord} g = r$ and $h \in H$ with $\operatorname{ord} h = s$. Then $\operatorname{ord}(g, h) = \operatorname{lcm}(r, s)$ in the direct product $G \times H$.*

Proof.

$$(g^e, h^e) = (g, h)^e = \mathbf{1} \text{ in } G \times H \Longleftrightarrow g^e = \mathbf{1} \text{ in } G \text{ and } h^e = \mathbf{1} \text{ in } H.$$

$\diamond$

Lemma 22 *Let G be a group with exponent r and H be a group with exponent s. Then the direct product $G \times H$ has exponent $t := \operatorname{lcm}(r, s)$.*

Proof. Since $r, s \mid t$ we have $(g, h)^t = (g^t, h^t) = (\mathbf{1}, \mathbf{1})$ for all $g \in G$ and $h \in H$. Thus the exponent e of $G \times H$ is $\leq t$.

Since $(\mathbf{1}, \mathbf{1}) = (g, h)^e = (g^e, h^e)$ for all g, h, we have $r \mid e$ and $s \mid e$, hence $t \mid e$. $\diamond$

Lemma 23 *Let G be a cyclic group of prime order r, and H, a cyclic group of prime order $s \neq r$. Then the direct product $G \times H$ is cyclic of order $r \cdot s$.*

Proof. Let $g \in G$ have order r, and $h \in H$ have order s. Then by Lemma 21 the element (g, h) has order $\operatorname{lcm}(r, s) = r \cdot s = \#(G \times H)$, hence generates $G \times H$. $\diamond$

Lemma 24 *Let G be an abelian group.*

(i) *Let $a, b \in G$, $\operatorname{ord} a = r$, $\operatorname{ord} b = s$, where r, s are finite and coprime. Then $\operatorname{ord}(ab) = rs$.*

(ii) *Let* $a, b \in G$, $\operatorname{ord} a = r$ *and* $\operatorname{ord} b = s$ *finite*, $t := \operatorname{lcm}(r, s)$. *Then* $\operatorname{ord}(ab) \mid t$, *and there is a* $c \in G$ *with* $\operatorname{ord} c = t$.

(iii) *Let* $m = \max\{\operatorname{ord} a \mid a \in G\}$ *be finite. Then* $\operatorname{ord} b \mid m$ *for all* $b \in G$. *In particular* m *is the exponent of* G.

Proof. (i) Let $k := \operatorname{ord}(ab)$. From $(ab)^{rs} = (a^r)^s \cdot (b^s)^r = \mathbf{1}$ we conclude that $k \mid rs$. Conversely, since $a^{ks} = a^{ks} \cdot (b^s)^k = (ab)^{ks} = \mathbf{1}$ we have $r \mid ks$, hence $r \mid k$, and likewise $s \mid k$, hence $rs \mid k$.

(ii) Let $k := \operatorname{ord}(ab)$. From $(ab)^t = a^t \cdot b^t = \mathbf{1}$ follows that $k \mid t$.

Now let p^e be a prime power with $p^e \mid t$, say $p^e \mid r$. Then a^{r/p^e} has order p^e. Let $t = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition with different primes p_i. Then there are $c_i \in G$ with $\operatorname{ord} c_i = p_i^{e_i}$. Since these orders are pairwise coprime, the element $c = c_1 \cdots c_r$ has order t by (i).

(iii) Let $\operatorname{ord} b = s$. Then by (ii) there is a $c \in G$ with $\operatorname{ord} c = \operatorname{lcm}(m, s)$. Hence $\operatorname{lcm}(m, s) \leq m$, hence $= m$, thus $s \mid m$. $\diamond$

Remarks

1. For non-abelian groups all three statements (i)–(iii) may be false. As an example consider the symmetric group $\mathcal{S}_4$ of order $4! = 24$. The possible orders of its elements are 1 (for the trivial permutation), 2 for permutations consisting of one or two disjoint 2-cycles, 3 for all 3-cycles, and 4 for all 4-cycles. Thus the maximum order is 4, but the exponent = the lcm of all orders is 12 (by Lemma 20). The cycle $\sigma = (1\,2\,3)$ has order $r = 3$, the transposition $\tau = (3\,4)$ has order $s = 2$. Their product is the 4-cycle $(2\,3\,4\,1)$ of order $4 \neq \operatorname{lcm}(r, s) = 6$, and there doesn't exist any permutation of order 6.

2. In a nontrivial abelian group the order of a product ab in general differs from the lcm of the single orders: Take $a \neq \mathbf{1}$ and $b = a^{-1}$.