Group Theory, 2016

Exercise sheet 3 (solutions)

Exercise 1. (a) Consider the map $\phi : G \to G,\ a \mapsto a^n$. Let us first see that this map is a homomorphism. This follows from

$$\phi(ab) = (ab)^n = a^n b^n = \phi(a)\phi(b).$$

Notice that we have used here the fact that G is abelian. By the first Isomorphism Theorem, we have that $\operatorname{im}\phi = G^n$ and $\ker\phi = G[n]$ are subgroups of G, and that $G/\ker\phi \cong \operatorname{im}\phi$. This gives us $G/G[n] \cong G^n$ as required.

(b) If $|r| > 1$ then $|r|^n > 1$ and if $|r| < 1$ then $|r|^n < 1$. It follows that the only rationals in $\mathbb{Q}^*$ of finite order are $1, -1$ of order 1 and 2 respectively. We consider two scenarios. If n is even then $G[n] = \{-1, 1\}$ and thus $G^n \cong G/\{-1, 1\}$. If on the other hand n is odd then $G[n] = \{1\}$ and $G^n \cong G/\{1\} \cong G$. There are thus only two groups up to isomorphism

$$G \cong G^1 \cong G^3 \cong ...$$

and

$$G/\{-1, 1\} \cong G^2 \cong G^4 \cong .....$$

Notice that the two groups are not isomorphic as G has an element, namely -1, of order 2 whereas G^2 has no element of order 2. (If $\phi : G \to G^2$ was an isomorphism then $\phi(-1)$ would be of order 2 in G^2).

Notice that $(\mathbb{C}^*)^n = \mathbb{C}^*$ and thus all powers of $\mathbb{C}^*$ are the same group. (If $u = re^{si}$ then for $v = \sqrt[n]{r}e^{\frac{s}{n}i}$ we have $v^n = u$).

Exercise 2. (a) Let $n = o(a)$. We have

$$(aN)^n = a^n N = 1N = N$$

hence the order of aN divides $n = o(a)$.

(b) By part (a), we have that $o(aN)$ divides $o(n)$. By Lagrange's Theorem, $o(aN) = |\langle aN\rangle|$ divides G/N. As G/N and $o(n)$ are coprime this implies that $o(aN) = 1$. That is $aN = N \Leftrightarrow a \in N$.

Exercise 3. No they are not isomorphic. To see this we argue by contradiction and we suppose that there is an isomorphism $\phi : \mathbb{Q} \to \mathbb{Q}^+$. Let $a \in Q$ be such that $\phi(a) = 2$. Then

$$2 = \phi(a/2 + a/2) = \phi(a/2)^2$$

and 2 has a rational square root $\phi(a/2)$. This is however absurd. Hence the groups can't be isomorphic.

Exercise 4. (a) We prove this by induction on $|G|$. The induction basis $|G| = 1$ obviously holds (as there is no prime that divides $|G|!$). Now suppose that $|G| \geq 2$ and that the result holds for all abelian groups of smaller order. Let a be a non-trivial element of G and let $H = \langle a \rangle$. Now $|G| = |H| \cdot |G/H|$ and thus p divides either $r = |H|$ or $s = |G/H|$. In the first case we have clearly an element of order p in G, namely $a^{r/p}$. Now consider the case when p divides $s = |G/H|$. As $s < n$, we have by induction hypothesis an element $[b] \in G/H$ of order p. Let m be the order of b in G. Then $[b]^m = [b^m] = [1]$ and thus the order of $[b]$, namely p, divides m. Now clearly the element $b^{m/p}$ is of order p in G. This finishes the proof of the induction step. $\Box$.

(b) We prove this by induction on $|G|$. The induction basis $|G| = 1$ is clear since G itself is a subgroup of order 1, the only m that divides $|G|$. Now suppose that $|G| \geq 2$ and that the result holds for all abelian groups of smaller order. Let m be a positive integer that divides $|G|$. If $m = 1$ we know that $H = \{1\}$ is a subgroup with m elements. Now suppose that $m \geq 2$ and let $m = rp$ for some prime p. By part (a) there is a subgroup H with p elments. Then $|G/H| < |G|$ and r divides $|G/H|$. By the induction hypothesis and the Correspondence Theorem there is a subgroup of G/H with r elements and this subgroup is of the form K/H where $H \leq K \leq G$. Then $|K| = |H| \cdot |K/H| = p \cdot r = m$ and we have found a subgroup K with m elements. This finishes the proof of the induction step. $\Box$.

Exercise 5. (a) We know that the set of all bijections from G to itself is a group. We show that $\mathrm{Aut}\,(G)$ is a group by showing that it is subgroup of the former. We need $\mathrm{id} : G \to G$ to be an automorphism and $\mathrm{Aut}(G)$ to be closed under composition and taking inverses. But this is easily checked and was done in lectures.

(b) Notice that ϕ_a is bijective with inverse $\phi_{a^{-1}}$. Also

$$\phi_a(xy) = axya^{-1} = axa^{-1} \cdot aya^{-1} = \phi_a(x) \cdot \phi_a(y)$$

that shows that ϕ_a is an automorphism. We next show that $\mathrm{Inn}(G)$ is a subgroup. To see this first notice that we have that $\mathrm{id} = \phi_e \in \mathrm{Inn}(G)$. Then as

$$\phi_a \circ \phi_b(x) = \phi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x)$$

and as $\phi_a^{-1} = \phi_{a^{-1}}$ we have that the required closure properties hold. So $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Finally to show that $\mathrm{Inn}\,(G)$ is a normal subgroup of $\mathrm{Aut}\,(G)$, notice that for any $\psi \in \mathrm{Aut}\,(G)$ and any $a \in G$ we have

$$\psi \circ \phi_a \circ \psi^{-1}(x) = \psi(a\psi^{-1}(x)a^{-1}) = \psi(a)x\psi(a)^{-1} = \phi_b(x)$$

where $b = \psi(a)$.

(c) We have

$$\Psi(a \cdot b) = \phi_{ab} = \phi_a \circ \phi_b = \Psi(a) \circ \Psi(b).$$

(d) Clearly $\mathrm{Im}(\Psi) = \mathrm{Inn}(G)$. Then $a \in \mathrm{Ker}(\Psi)$ iff $\phi_a = \mathrm{id}$ iff $\phi_a(x) = x$ for all $x \in G$. But this holds iff $axa^{-1} = x$ for all $x \in G$ that is to say iff $ax = xa$ for all $x \in G$. So $a \in \mathrm{Ker}(\Psi)$ iff $a \in Z(G)$. The 1st isomorphism theorem tells us that

$$\mathrm{Inn}(G) = \mathrm{Im}(\Psi) \cong G/\mathrm{Ker}(\Psi) = G/Z(G).$$