MATH 8510, Abstract Algebra I
Fall 2016
Exercises 5-1
Shuai Wei

Exercise 1. Let G be a group.

(a) (3.1.36) Prove that if $G/Z(G)$ is cyclic, then G is abelian. (See the hint in the text.)

Proof. At first, we show $Z(G) \trianglelefteq G$.
We already know $Z(G) \leq G$. Besies, since
$\forall g \in G, z \in Z(G), gz = zg$ by the definition of $Z(G)$,

$$gzg^{-1} = zgg^{-1} = z \in Z(G), \forall g \in G, z \in Z(G)$$

Thus,

$$Z(G) \trianglelefteq G.$$

Since $G/Z(G)$ is cyclic, there exist $x \in G$ such that $G/Z(G) = \langle xZ(G) \rangle$.
Next we show every element of G can be written in the form $x^a z$ for some integer $a \in Z$ and some element $z \in Z(G)$.
Then $\forall g \in G$, there exists $n \in \mathbb{Z}$ such that

$$gZ(G) = \big(xZ(G)\big)^n = x^n Z(G)$$

since $Z(G) \trianglelefteq G$.
Then

$$(x^n)^{-1} g \in Z(G).$$

So there exists $z \in Z(G)$ such that

$$(x^n)^{-1} g = z$$

Thus,

$$g = x^n z$$

At last, we have $\forall g, h \in G$, there exists $m, n \in Z, y, z \in Z(G)$ such that

$$g = x^m y, \text{ and } h = x^n z,$$

and we have

$$\begin{aligned} gh &= x^m y x^n z \\ &= x^m x^n y z \\ &= x^{m+n} z y \\ &= x^{n+m} z y \\ &= z x^{n+m} y \\ &= z x^n x^m y \\ &= x^n z x^m y \\ &= hg \end{aligned}$$

So G is abelian.

$\square$

(b) (3.2.4) Prove that if $|G| = pq$ where p and q are (not necessarily distinct) primes, then either G is abelian or $Z(G) = \{e\}$.

Proof. We first show that if H is a group and $|H| = p$, where p is a prime, then G is cyclic.
Let $x \in H$ and $x \neq 1$, then $|x| \neq 1$ and $|x| \mid |H|$.
So $|x| = p$ and then $langlex\rangle = H$.
Thus, H is cyclic.
Since $Z(G) \leq G$, $Z(G)| \mid |G|$.
Given $|G| = pq$ and p, q are primes, we have $|Z(G)| = 1$ or p, q or pq.

(i) If $|Z(G)| = 1$, then $Z(G) = \{e\}$.
(ii) If $|Z(G)| = pq$, we know $Z(G) \leq G$ and then $Z(G) = G$.
So $\forall h \in Z(G)$, we have $h \in G$ arbitrary and

$$hg = gh, \forall g \in G.$$

by the definition of $Z(G)$.
Thus G is abelian.
(iii) If $|Z(G)| = p$, we have

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = q.$$

Since q is a prime, $G/Z(G)$ is cyclic by the previous proof.
Thus, G is abelian according to part (a).
(iv) If $|Z(G)| = q$, follow the similar process as (iii), we have G is abelian.

In summary, if $|G| = pq$ where p, q are primes, then either G is abelian or $Z(G) = e$.

□

Exercise 2 (Bonus, 3.2.9)**.** Prove Cauchy's Theorem: If G is a finite group and p is a prime number such that $p \mid |G|$, then there is an element $x \in G$ such that $|x| = p$. (Note that the text includes an outline of a proof in Exercise 3.2.9.)

Proof. Let

$$S = \{(x_1, x_2, ...x_p) | x_i \in G \text{ and } x_1x_2...x_p = 1\}.$$

(1) At first, we show $|S| = |G|^{p-1}$.
Let $x_i, i = 1, 2, ...p-1$ be any element of G, then $x_p = x_1^{-1}x_2^{-1}...x_{p-1}^{-1}$.
Namely, $x_i, i = 1, 2, ...p-1$ has $|G|$ choices each, and then x_p only has one.
So $|S| = |G|^{p-1}$.
Define a relation $\sim$ on S by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.
(2) Then we show a cyclic permutation of an element of S is again an element of S.
$\forall s = (x_1, x_2, ...x_p) \in S$, we have $x_1x_2...x_p = 1$.
Define

$$r : S \to S$$

$$(x_1, x_2, ...x_p) \mapsto (x_p, x_1, ...x_{p-1})$$

Since $(x_1, x_2, ...x_p) \in G$, $x_1x_2...x_p = 1$.
So $x_px_1x_2...x_{p-1}x_p^{-1} = x_p1x_p^{-1}$.
Namely, $x_px_1...x_{p-1} = 1$. So $(x_p, x_1, ...x_{p-1}) \in S$.

Thus, f is well-defined.
Similarly, define

$$l : S \to S$$
$$(x_1, x_2, ...x_p) \mapsto (x_2, x_3...x_p, x_1)$$

which is well-defined.
Hence, a cyclic permutation of an element of S is again an element of S.

(3) Next we show $\sim$ is an equivalence relation.

  (a) By the definition of r and l, we have $r^p = e_r$ and $l^p = e_l$.
  Then $\forall s \in S, r^p(s) = e_r(s) = s$.
  So $s \sim s$.
  (b) $\forall s, t \in S$,if $s \sim t$, without loss of generality, assume $s = r^n(t)$ for some $n \in \mathbb{Z}$. Then $t = l^n(s)$. As a result, $t \sim s$.
  (c) Let $s, t, v \in G$ and $r \sim s$ and $s\ t$.
  Without loss of generality, assume $s = r^m(t)$ and $t = l^n(v)$ for some $m, n \in \mathbb{Z}$.
  Then $s = r^m(l^n(v)) = r^{m-n}(v)$ if $m \geq n$ or $s = l^{n-m}(v)$ if $m < n$.
  So $s \sim v$.

Thus, $\sim$ is an equivalence relation.

(4) Then we show an equivalence class contains a single element if and only if it is of the form $(x, x, ..., x)$ with $x^p = 1$.
Assume an equivalence class contains a single element $s = (x_1, x_2, ..., x_p)$ with $x_1 x_2 ... x_p = 1$.
Then $s = l(s) = l^2(s) = ... = l^{p-1}(s)$.
Look at the first element of $s, l(s), l^{p-1}(s)$, we have $x_1 = x_2 = ... = x_p$.
Therefore, such a element is of the form $s = (x, x, ..., x)$ with $x^p = 1$.
Assume an equivalence class contains the element which is of the form $s = (x, x, ..., x)$ with $x^p = 1$.
Then $l^n(s) = r^n(s) = s$ for any $n \in \mathbb{Z}$.
Thus, the equivalence only contains the single element $s = (x, x, ..., x)$.

□

Exercise 3 (3.3.7)**.** Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$.