MATH 8510, Abstract Algebra I
Fall 2016
Exercises 5-1
Shuai Wei
Collaborator: Xiaoyuan Liu

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,

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

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 $z \in Z(G)$.
Since $G/Z(G)$ is cyclic, there exist $x \in G$ such that $G/Z(G) = \langle xZ(G)\rangle$.
$\forall g \in G$, $gZ(G) \in G/Z(G)$, so there exists some $n \in \mathbb{Z}$ such that

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

using $Z(G) \trianglelefteq G$.
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

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

since $y, z \in Z(G)$.
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 $\langle x \rangle = H$.
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 problem (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 $Z(G) = \{e\}$.

$\square$

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 $s = (x_1, x_2, ...x_p) \in S$ and $x_i, i = 1, 2, ...p-1$ be any element of G, then $x_p = x_{p-1}^{-1}x_{p-2}^{-1}...x_1^{-1}$.
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
$$\pi : S \to S$$
$$(x_1, x_2, ...x_p) \mapsto (x_p, x_1, ...x_{p-1})$$
Then we define π as circular shift operation.
Since $(x_1, x_2, ...x_p) \in G$, $x_1x_2...x_p = 1$.
So $x_px_1x_2...x_{p-1}x_px_p^{-1} = x_p1x_p^{-1}$.

Namely, $x_p x_1 ... x_{p-1} = 1$. So $(x_p, x_1, ...x_{p-1}) \in S$.
Thus, π 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.
Then we have a group $G = \langle \pi \rangle$ acting on the set S.
Thus, it is obvious $\sim$ 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 $\pi = \pi(s) = \pi^2(s) = ... = \pi^{p-1}(s)$.
Look at the first element of all the elements $s, \pi(s), ..., \pi^{p-1}(s)$, 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 it is obvious that $\pi^n(s) = s$ for $1 \leq n \leq p, n \in \mathbb{Z}$.
Thus, the equivalence only contains the single element $s = (x, x, ..., x)$.

(5) Then we show every equivalence class has order 1 or p. Let $G = \langle \pi \rangle$.
Then $|G| =$ p. The orbits of S under the action of G form a partion of S.
Let $s \in S$, then its stabilizer $G_s \leq G$.
So $|G_s| = 1$ or p by Lagrange's theorem.
Let $\mathcal{O}(s)$ denote the orbit containing s.
  (a) If $|G_s| = p$, then $G_s = G$.
  So $s = (g, g, ...g)$ for some $g \in G$ since s stays the same under all the $\pi, \pi^2, ...\pi^p$ circular shift operations.
  By part (d), $\mathcal{O}(s)$ has order 1.
  (b) If $|G_s| = 1$, then $G_s = \{e_G\}$.
  Assume $|\mathcal{O}(s)| < p$, then there exists some $n \in \mathbb{Z}$ and $1 \leq n \leq p - 1$ such that $s = \pi^n(s)$.
  Then $e_G \neq \pi^n \in G_s$, which is contrdicted by $|G_s| = 1$.
  So $|\mathcal{O}(s)| = p$ since $|\mathcal{O}(s)| \leq p$.

Let k be the number of classes of size 1 and d be the number of classes of size p.
Since S is the disjoint union of its orbits, we have $|S| = |G|^{p-1} = k + pd$.

(6) By part(c), we have $\{(1, 1, .., 1)\}$ is an equivalence class of size 1, and then $k \geq 1$.
Since S has order divisible by p by part (a), we have $k \geq p \geq 2$.
So there is another element x different from $(1, 1, ..., 1)$ which has order p.
Then by part (d), we have $x \in S$ is of the form $(x, x, ..., x)$ with $x^p = 1$.

□

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

Proof. Define f as

$$\begin{aligned} f : G &\to (G/M) \times (G/N) \\ g &\mapsto (gM, gN) \end{aligned}$$

$\forall g, h \in G$,

$$f(gh) = (ghM, ghN) = (gMhM, gNhN) = (gM, gN)(hM, hN)$$

So f is a homomorphism.

$$\begin{aligned} g \in \mathrm{Ker}(f) &\Leftrightarrow f(g) = (M, N),\ \forall g \in G \\ &\Leftrightarrow (gM, gN) = (M, N),\ \forall g \in G \\ &\Leftrightarrow gM = M \text{ and } gN = N,\ \forall g \in G \\ &\Leftrightarrow g \in M \text{ and } g \in N,\ \forall g \in G \\ &\Leftrightarrow g \in M \cap N,\ \forall g \in G \end{aligned}$$

So

$$\mathrm{Ker}(f) = M \cap N.$$

Let $(gM, hN) \in (G/M) \times (G/N)$, then there exist $m_1, m_2 \in M$, $n_1, n_2 \in N$ such that $g = m_1 n_1$ and $h = m_2 n_2$ since $G = MN$.
Since $M \trianglelefteq G$ and $N \trianglelefteq G$,

$$\begin{aligned} (gM, hN) &= (m_1 n_1 M, m_2 n_2 N) \\ &= (n_1 n_1^{-1}) m_1 n_1 M, m_2 n_2 (m_2^{-1} m_2) N) \\ &= n_1 (n_1^{-1} m_1 n_1) M, (m_2 n_2 m_2^{-1}) N m_2) \\ &= (n_1 M, N m_2) \\ &= (n_1 M, m_2 N) \\ &= (n_1 (n_1^{-1} m_2 n_1) M, m_2 n_1 N) \\ &= (m_2 n_1 M, m_2 n_1 N) \\ &= f(m_2 n_1). \end{aligned}$$

So f is onto. Namely, $\mathrm{Im}(f) = (G/M) \times (G/N)$.
Thus, by the first isomorphism theorem, we have

$$G/(M \cap N) \cong (G/M) \times (G/N).$$

$\square$