MATH 410 Homework 7

Qilin Ye

April 1, 2021

3.6.14 In $\mathbb{Z}/60\mathbb{Z}$, the only element of order 2 is $[30]$. (Obvious enough — if $2k \equiv 0 \pmod{60}$ for $0 \leqslant k \leqslant 59$ and $k \not\equiv 0 \pmod{60}$ then the only possibility is if $k = 30$.) Likewise, the only two elements of order 3 are $[20]$ and $[40]$ (which correspond to $60/3$ and $60 \cdot 2/3$). There are 2 elements of order 4: $[15]$ and $[45]$ which correspond to $60/4$ and $60 \cdot 3/4$. (Note that $60 \cdot 2/4 = 30$ but $o[30] = 2$.) 4 elements of order 5: $[12], [24], [36]$, and $[48]$.

In $\mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$[1], things become slightly more complicated. Recall that $o(x,y) = \operatorname{lcm}(o(x), o(y))$. If an element has order 2 then $(o(x), o(y))$ can be $(1,2), (2,1)$ or $(2,2)$. These correspond to $(0,1), (15,0)$, and $(15,1)$, respectively. Thus 3 elements have order 2.

For order 3, $(o(x), o(y))$ can be $(1,3), (3,1)$, or $(3,3)$. Of course by Lagrange's theorem $o(y) \mid 2$ so this can only happen if $o(x) = 3$ and $o(y) = 1$, namely the ordered pairs $(10,0)$ and $(20,0)$, two elements.

For order 4, if we want $\operatorname{lcm}(m,n) = 4$ then either $m = 4$ or $n = 4$. However, neither one can be true because $4 \nmid 30$ and $4 \nmid 2$. Thus no element has order 4. For order 5, immediately we see $o(y) = 1$ and $o(x) = 5$. This simply corresponds to $(6,0), (12,0), (18,0)$, and $(24,0)$. Four elements.

3.6.19 If $\gcd(m,n) = 1$ then T is in fact a bijection, as the Chinese remainder theorem guarantees that

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}$$

corresponds to precisely one $0 \leqslant c \leqslant mn - 1$ such that $x \equiv c \pmod{mn}$. It is also clear that T defines a homomorphism since

$$T(xy) = ([xy]_m, [xy]_n) = ([[x][y]]_m, [[x][y]]_n) = T(x)T(y). \qquad \square$$

3.7.7 We verify the two criteria. Let $g_1, g_2 \in G$ be given. It follows that

$$(g_2 g_1) \cdot x = g_2 g_1 x g_1^{-1} g_2^{-1} = g_2(g_1 x g_1^{-1}) g_2^{-1} = g_2 \cdot (g_1 \cdot x),$$

and taking $g := e \in G$ gives $gxg^{-1} = exe^{-1} = x$ for all $x \in G$. $\square$

3.7.8 Let $\sigma, \tau \in \operatorname{Stab}(x)$. It follows that $\sigma x = \tau x = x$. Then

$$(\sigma\tau)x = \sigma(\tau x) = \sigma x = x \implies \sigma\tau \in \operatorname{Stab}(x)$$

and

$$x = \tau^{-1}\tau x = \tau^{-1}(\tau x) = \tau^{-1} x \implies \tau^{-1} \in \operatorname{Stab}(x).$$

The claim then follows from the two-step subgroup test.

[1] I'd like to thank Alan Goldfarb for pointing out my mistake: I mistakenly used $\mathbb{Z}/60\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and got some wrong results.

3.7.9 The orbit consists of all possible values of form $x_{\sigma(1)}x_{\sigma(3)} - x_{\sigma(2)}x_{\sigma(4)}$. Since $x_i x_j = x_j x_i$, order within pair does not matter. Hence there are 4 choose 2 elements in the orbit, namely

$$x_1x_2 - x_3x_4, x_1x_3 - x_2x_4, x_1x_4 - x_2x_3, x_2x_3 - x_1x_4, x_2x_4 - x_1x_3, x_3x_4 - x_1x_2.$$

The stabilizer of P will at most permute x_1 with x_3 and x_2 with x_4. Thus

$$\text{Stab}(P) = \{e, (13), (24), (13)(24)\}.$$

3.7.14 Per the discussion we first prove the statement in Ex.3.6.12.

Proposition

If $H \triangleleft G, K \triangleleft G$ and $H \cap K = \{e\}$, then the map $T : HK \to H \oplus K$ defined by $hk \mapsto (h, k)$ is a well-defined group isomorphism.

Proof. We show well-definedness, injectivity, surjectivity, and structure preservation one by one.

(1) T is well-defined: suppose $h_1k_1, h_2k_2 \in HK$ and $h_1k_1 = h_2k_2$. Then $(h_1k_1)k_1^{-1} = (h_2k_2)k_1^{-1}$ and so

$$\underbrace{h_1}_{\in H} = \underbrace{h_2}_{\in H}\underbrace{(k_2k_1^{-1})}_{\in K}.$$

By closure of group we are forced to the conclusion that $k_2k_1^{-1} \in H$. Thus by assumption $k_2k_1^{-1}$ is in $H \cap K = \{e\}$, i.e., $k_2 = k_1$. Clearly $h_1 = h_2$ as well, so $T(h_1k_1) = (h_1, k_1) = (h_2, k_2) = T(h_2k_2)$.

(2) T is injective: if $(h_1, k_1) = (h_2, k_2)$ then $h_1 = h_2, k_1 = k_2 \implies h_1k_1 = h_2k_2$.

(3) T is surjective: obvious; for $(h, k) \in H \oplus K$ we have $(h, k) = T(hk)$ where $h \in H, k \in K$, so $hk \in HK$.

(4) T preserves group structure: we want to show that, for all $h_1k_1, h_2k_2 \in HK$,

$$T(h_1k_1 \cdot h_2k_2) = T(h_1k_1)T(h_2k_2).$$

Notice that

$$T(h_1k_1)T(h_2k_2) = (h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2),$$

so it suffices to show $h_1k_1h_2k_2 = h_1h_2k_1k_2$ and in particular $k_1h_2 = h_2k_1$. This in fact holds given normality of H, K. Consider $g := (k_1h_2)(k_1^{-1}h_2^{-1})$. Writing it as $(k_1h_2k_1^{-1})h_2^{-1}$ we see $k_1h_2k_1^{-1} \in H$ and so $g \in H$. Likewise, writing g as $k_1(h_2k_1^{-1}h_2^{-1})$ suggests $g \in K$. Therefore $g = e$, i.e.,

$$k_1h_2 = (k_1^{-1}k_2^{-1})^{-1} = k_2h_1.$$

We've shown that T indeed defines a group isomorphism $HK \to H \oplus K$. □

Back to Ex.3.7.14: per the discussion, since $|A| = 3$, $|B| = 5$, and both are cyclic, there exists an (in fact much more than one) element $(a, b) \in A \oplus B$ such that $o((a, b)) = \text{lcm}(3, 5) = 15$. The isomorphism between $A \oplus B$ and AB guarantees that there also exists an element $g \in AB$ with order 15. Clearly $AB \subset G$ so $o(g) = 15$ with respect to G. Since $|G| = 15$ itself, we conclude that $G = \langle g \rangle$, i.e., any group of order 15 is cyclic. □

3.7.26 If $G/Z(G)$ is cyclic, then there exists $g \in G$ such that $G/Z(G) = \langle gZ(G) \rangle$.

Claim: any $a \in G$ is of form $g^m z$ for some integer m and $z \in Z(G)$. To see this, first write $aZ(G)$ as $(gZ(G))^m$. By definition, this means $aZ(G) = g^m Z(G)$. It follows that $(g^m)^{-1}a = g^{-m}a \in Z(G)$ and so $g^{-m}a = z$ for some $z \in Z(G)$. Thus $a = g^m z$, as desired.

Back to the main proof: now we pick arbitrary $h, k \in G$. It follows that $h = g^x z_1$ and $k = g^y z_2$ for integers x, y and some $z_1, z_2 \in Z(G)$. The remainder of this proof is simply a chain of equations:

$$hk = g^x z_1 g^y z_2 = g^x g^y z_1 z_2 = g^y g^x z_2 z_1 = g^y z_2 g^x z_1 = kh,$$

i.e., G is abelian. $\square$