THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2023-24
Tutorial 4 solutions
5th October 2023

- The tutorial solutions are written for reference and proofs will be sketched briefly. You should try to fill in the details as an exercise. The solutions for Homework optional questions can be found in Homework solutions, which would be released after the deadlines. Please send an email to echlam@math.cuhk.edu.hk if you have any further questions.

1. Since $\mathbb{Z}_p$ is cyclic, fix the generator $1 \in \mathbb{Z}_p$, then every automorphism $f \in \operatorname{Aut}(\mathbb{Z}_p)$ is determined by where it sends the generator 1 to. Recall that there are $\phi(p) = p-1$ many generators of $\mathbb{Z}_p$ corresponding to the number of integers that are coprime to p, where ϕ is the Euler totient function. In other words, for each $k = 1, ..., p-1$, $f_k(1) := k$ determines an automorphism of $\mathbb{Z}_p$. Now given k_1, k_2, notice that $f_{k_1} \circ f_{k_2}(1) = k_1 k_2 \mod p$. Now let $\mathbb{Z}_p^\times$ denotes the multiplicative group of units of (the ring) $\mathbb{Z}_p$, i.e. it consists of elements in $\{0, 1, 2, ..., p-1\}$ that are invertible. By Fermat's little theorem, every nonzero element in $\mathbb{Z}_p$ admits a multiplicative inverse, so that $\mathbb{Z}_p^\times = \mathbb{Z}_p - \{0\}$ as set. As such, we may define $F : \mathbb{Z}_p^\times \to \operatorname{Aut}(\mathbb{Z}_p)$ by $k \mapsto f_k$. It is a group homomorphism since $F(i \cdot j) : 1 \mapsto ij$ and $F(i) \circ F(j) : 1 \mapsto i \cdot j$ are equal. Then F is an isomorphism since it is injective and both groups have order $p-1$. Finally, $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$ holds true according to Fermat's little theorem again, since any $k \in \{1, ..., p-1\}$ is a cyclic generator.

   For $\mathbb{Z}$, similar to above it is generated by 1, therefore we just needs to send it to other generators. But $\mathbb{Z}$ only has two generators $\{1, -1\}$. Therefore $\operatorname{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$. Finally for $\mathbb{Z}^2$ it is more complicated. It has standard generators $\{(1,0), (0,1)\}$. To determine $f \in \mathbb{Z}^2$ is to determine what are pairs of generators of $\mathbb{Z}^2$. Notice that if $(a, b), (c, d)$ is a set of generators of $\mathbb{Z}^2$, then we can generate $(1, 0), (0, 1)$ from them, therefore there are $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ so that
$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
   In other words, $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is an invertible matrix with integer coefficients. Furthermore, composition of two automorphisms corresponds to multiplication of matrix. Concretely, what we have is an isomorphism $GL_2(\mathbb{Z}) \to \operatorname{Aut}(\mathbb{Z}^2)$ where we associate to each matrix $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ the automorphism $f_A : (1,0) \to (a,b)$ and $f_A : (0,1) \to (c,d)$.

2. First notice that $Tg \cdot T(g^{-1}) = T(gg^{-1}) = Te = e$ implies that $T(g^{-1}) = (Tg)^{-1}$. Since G is a finite group, to show that $g \mapsto g^{-1}Tg$ is surjective amounts to showing that it is injective. Suppose that $g^{-1}Tg = h^{-1}Th$, then we have $gh^{-1} = Tg(Th)^{-1} = TgT(h^{-1}) = T(gh^{-1})$. By assumption this implies $gh^{-1} = e$, so $g = h$ and the map $g \mapsto g^{-1}Tg$ is indeed injective.

3. Following question 3, we know that any $h \in G$ can be expressed as $g^{-1}Tg$. If $T^2 = \mathrm{Id}$, then $Th = T(g^{-1}) \cdot T^2(g) = T(g^{-1})g = (g^{-1}Tg)^{-1} = h^{-1}$ for any $h \in G$. So T is simply given by inverting an element, however if this is indeed a automorphism, then for

arbitrary, h_1, h_2, $T(h_1 h_2) = h_2^{-1} h_1^{-1}$, meanwhile $Th_1 Th_2 = h_1^{-1} h_2^{-1}$. This shows that G is automatically abelian.

4. Recall that the dihedral group D_{2n} can be generated by a rotation r and a reflection s, subject to the condition that $r^n = e$, $s^2 = e$, and $rsrs = e$. Alternatively, you can just think of r as rotation by $2\pi/n$ counterclockwise, and s as just a reflection about some diagonal of the regular n-gon. The relation $rsrs = e$ geometrically just means that rs is again a reflection, and we can rewrite it as $rs = sr^{-1} = sr^{n-1}$. Then inductively one can see $r^k s = sr^{n-k}$. This equation already tells us that r^k is not in the center of D_{2n} unless $k = n - k$, this forces $n = 2k$ to be even.

   As for reflection elements in D_{2n}, they can be written as $r^k s$ for $k = 0, ..., n-1$. Then consider $(r^k)sr = r^k r^{-1} s \neq r^{k+1} s$. This shows that $r^k s \notin Z(D_{2n})$ as well. Therefore we conclude that

$$Z(D_{2n}) = \begin{cases} 1, & \text{if } n \text{ is odd.} \\ \{e, r^{n/2}\}, & \text{if } n \text{ is even.} \end{cases}$$

5. There is an obvious map $\varphi : H \times K \to G$ by $\varphi(h,k) = hk \in G$. The claim is that this is a group isomorphism. Recall from tutorial 3 question that $hk = kh$ for any $h \in H$ and $k \in K$ because $hkh^{-1}k^{-1} \in H \cap K = \{e\}$. Therefore $\varphi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \varphi(h_1, k_1)\varphi(h_2, k_2)$, and $\varphi(e,e) = ee = e$ so φ is a well-defined homomorphism. This is surjective by the condition that any $g \in G$ can be written as $g = hk = \varphi(h,k)$. It is injective because $\varphi(h,k) = hk = e$ implies that $h = k^{-1} \in H \cap K = \{e\} \Rightarrow h = k = e$.