THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2019-20
Homework 1 Solution
Due Date: 12th September 2019

Compulsory part

1. Let $S = \{x \in G : x^{-1} \neq x\}$. Then S has an even number of elements, because the elements can be grouped in pairs x, x^{-1}. Because G has an even number of elements, the set $G - S$ must carry even number of element. Furthermore the set $G - S$ is nonempty because it contains e. Thus there is at least one element of $G - S$ other than the identity e, that is, at least one element other than e such that its own inverse is just itself.

2. Consider $(a * b) * (a * b)$. From the given condition: $x * x = e$ for all $x \in G$, we have $e = (a * b) * (a * b)$, and also $(a * a) * (b * b) = e * e = e$. Thus

$$a * b * a * b = e = a * a * b * b.$$

By cancellation, one has $b * a = a * b$.

3. Let $a \in H$ and let H have n elements. Then we find that the elements $a, a^2, a^3, \cdots, a^{n+1}$ are all in H as H is closed under the operation and observe that the elements cannot all be different, so $a^i = a^j$ for some $i < j$. Then we have $e = a^{j-i}$ so $e \in H$. Also, $a^{-1} \in H$ because $a^{-1} = a^{j-i-1}$. This shows that H is a subgroup of G.

4.
   - Closure: Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Because H and K are both subgroups of G, we have $ab \in H$ and $ab \in K$, so $ab \in H \cap K$.
   - Identity: As $e \in H$ and $e \in K$, $e \in H \cap K$.
   - Inverse: Let $a \in H \cap K$. Then $a \in H$ and $a \in K$. Because H and K are both subgroups of G, we have $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$.

5. Note that every group is the union of its cyclic subgroups, because every element of the group generates a cyclic subgroup that contains the element. Let G have only a finite number of subgroups, and hence only a finite number of cyclic subgroups. Now none of these cyclic subgroups can be infinite, for every infinite cyclic group is isomorphic to $\mathbb{Z}$ which contains infinitely of subgroups. Such subgroups of an infinite cyclic subgroup of G would of course give an infinite number of subgroups of G, contrary to hypothesis. Thus G can only have a finite number of finite cyclic subgroups. One leads that the set G can be written as a finite union of finite sets, so G is itself a finite set.

6. The positive integers less that pq and relatively prime to pq are those that are not multiples of p and are not multiples of q. Note that there are $p-1$ multiples of q and $q-1$ multiples of p that are less than pq. Thus there are $(pq-1)-(p-1)-(q-1) = pq-p-q+1 = (p-1)(q-1)$ positive integers less than pq and relatively prime to pq.

7.
$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix} \neq \begin{pmatrix}2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix}$$

8. Let $A = \{a_1, a_2, \ldots, a_n\}$. Consider the permutation $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$. Clearly $\sigma \in S_n$. Note that $|\sigma| = n$ and hence $H := \langle \sigma \rangle$ is a cyclic group of order $n(= |A|)$. This group H is transitive on A as $\sigma^{j-i}(a_i) = a_j$ for any $1 \le i, j \le n$.

9. (a) Note that a cycle of length n can be written as a product of $n-1$ transpositions as

$$\begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & n \end{pmatrix} \begin{pmatrix} 1 & n-1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}.$$

   Now a permutation in S_n can be written as a product of disjoint cycles, the sum of whose lengths is $\le n$. If there are r disjoint cycles involved, we see the permutation can be written as a product of at most $n - r$ transpositions. Because $r \ge 1$, we can always write the permutation as a product of at most $n - 1$ transpositions.

   (b) It follows immediately from our proof of (a), because we must have $r \ge 2$.

   (c) Write the odd permutation σ as a product of s transpositions, where $s \le n - 1$ by Part(a). Then s is an odd number and $2n + 3$ is an odd number, so $2n + 3 - s$ is an even number. Adjoin $2n + 3 - s$ transpositions $\begin{pmatrix} 1 & 2 \end{pmatrix}$ as factors at the right of the product of the s transpositions that comprise σ. The same permutation σ results as $\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} = id$. Thus σ can be written as a product of $2n + 3$ permutations.

   If σ is even, we proceed in exactly the same way, but this time s is even so $2n+8-s$ is also even. We tack the identity permutation, written as a product of the $2n+8-s$ factors $\begin{pmatrix} 1 & 2 \end{pmatrix}$, onto the end of σ and obtain σ as a product of $2n + 8$ transpositions.

10. Suppose $\sigma \in H$ is an odd permutation. Let $\phi : H \to H$ be defined by $\phi(\mu) = \sigma\mu$ for $\mu \in H$. If $\phi(\mu_1) = \phi(\mu_2)$, then $\sigma\mu_1 = \sigma\mu_2$, so $\mu_1 = \mu_2$ by group cancellation. Also, for any $\mu \in H$, we have $\phi(\sigma^{-1}\mu) = \sigma\sigma^{-1}\mu = \mu$. This shows that ϕ is a one-to-one map of H onto itself. Because σ is an odd permutation, we see that ϕ maps an even permutation onto an odd one, and an odd permutation onto an even one. Because ϕ maps the set of even permutations in H one to one onto the set of odd permutations in H, it is immediate that H has the same number of even permutations as odd permutations. Thus we have shown that if H has one odd permutation, it has the same number of even permutations as odd permutations.

Optional Part

1. First of all, it is not difficult to see that$\langle G, * \rangle$ is a group, because the order of multiplication in G is simply reversed: $(a*b)*c = a*(b*c)$ follows at once from $c\cdot(b\cdot a) = (c\cdot b)\cdot a$, the element e is still the identity element, and also the inverse of each element remains the same.

   Let $f(a) = a^{-1}$ for $a \in G$, where a^{-1} is the inverse of a in the group $\langle G, \cdot \rangle$. Uniqueness of inverses and the fact that $(a^{-1})^{-1} = a$ show at once that f is one to one and onto G. Also,

$$f(a \cdot b) = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = a^{-1} * b^{-1} = f(a) * f(b),$$

   showing that f is an isomorphism of $\langle G, \cdot \rangle$ onto $\langle G, * \rangle$.

2. Let G be a group with no proper nontrivial subgroups. If $G = \{e\}$, then G is of course cyclic. If $G \neq \{e\}$, then there is $a \in G$, such that $a \neq e$. We know that $\langle a \rangle$ is a subgroup of G and $\langle a \rangle \neq \{e\}$. Because G has no proper nontrivial subgroups, we must have $\langle a \rangle = G$, so G is indeed cyclic.

3. (a) Let a be a generator of H and let b be a generator of K. Because G is abelian, we have

$$(ab)^{rs} = (a^r)^s (b^s)^r = e^r e^s = e.$$

We claim that no lower power of ab is equal to e, for suppose that $(ab)^n = a^n b^n = e$. Then $a^n = b^{-n} = c$ must be an element of both H and K, and thus the order of c divides r and s. Because r and s are relatively prime, we see that we must have $c = e$, so $a^n = b^n = e$. But then n is divisible by both r and s, and because r and s are relatively prime, we have $n \geq rs$. Thus ab generates the desired cyclic subgroup of G of order rs.

(b) Let L the least common multiple of r and s. Using prime factorization, $L = \prod_{i=1}^{k} p_i^{r_i}$ where p_i is prime and $r_i \in \mathbb{Z}^+$. If we can find an element of G with order $p_i^{r_i}$ for every i, then by the above, the product of these elements would have order L because prime powers are all relatively prime to prime powers of different primes. Fix i. It suffices to find an element having order $p_i^{r_i}$. We know that $p_i^{r_i}$ is divisible by r or s. WLOG, we suppose $p_i^{r_i} | r$. Let a be a generator of H. Then $a^{m/p_i^{r_i}}$ has order $p_i^{r_i}$.

4. (a) Note that the $n \times n$ permutation matrices form a subgroup of the group $GL(n, \mathbb{R})$ of all invertible $n \times n$ matrices under matrix multiplication.

Let us number the elements of G from 1 to n, and number the rows of I_n from 1 to n, say from top to the bottom in the matrix. We can associate with each $g \in G$ a permutation (reordering) of the elements of G, which we can now think of as a reordering of the numbers from 1 to n, which we can in turn think of as a reordering of the rows of the matrix I_n, which is in turn produced by multiplying In on the left by a permutation matrix P. The effect of left multiplication of a matrix by a permutation matrix, explained in the exercise, shows that this association of g with P is an isomorphism of G with a subgroup of the group of all permutation matrices.

(b) We number the elements $e, a, b,$ and c of the Klein 4-group in Table 5.11 with the numbers $1, 2, 3,$ and 4 respectively. Performing the left multiplication, we can have the following correspondence:

$$e \leftrightarrow I_4, a \leftrightarrow \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \ b \leftrightarrow \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \ c \leftrightarrow \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

5. Note that

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \end{pmatrix}^r \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \cdots & n \end{pmatrix}^{n-r} = \begin{cases} \begin{pmatrix} 1 & 2 \end{pmatrix} & \text{for } r = 0, \\ \begin{pmatrix} r+1 & r+2 \end{pmatrix} & \text{for } r = 1, 2, \ldots, n-2, \\ \begin{pmatrix} n & 1 \end{pmatrix} & \text{for } r = n-1. \end{cases}$$

For $r = 0$ or $n - 1$, it is trivial. For $r = i$ with $1 \leq i \leq n - 2$, $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \end{pmatrix}^{n-i}$ maps $i + 1$ to 1, which is then mapped into 2 by $\begin{pmatrix} 1 & 2 \end{pmatrix}$, which is mapped into $i + 2$

by $\begin{pmatrix}1 & 2 & 3 & \cdots & n\end{pmatrix}^i$. By a similar manner, $i+2$ maps to $i+1$. For the others, it is unchanged.

Let $\begin{pmatrix}i & j\end{pmatrix}$ be any transposition, written with $i<j$. We observe that

$$\begin{pmatrix}i & j\end{pmatrix} = \begin{pmatrix}i & i+1\end{pmatrix} \cdots \begin{pmatrix}j-2 & j-1\end{pmatrix} \begin{pmatrix}j-1 & j\end{pmatrix} \begin{pmatrix}j-2 & j-1\end{pmatrix} \cdots \begin{pmatrix}i & i+1\end{pmatrix}.$$

By Corollary 9.12, every permutation in S_n can be written as a product of transpositions, which we now see can each be written as a product of the special transpositions $\begin{pmatrix}1 & 2\end{pmatrix}$, $\begin{pmatrix}2 & 3\end{pmatrix}$, ..., $\begin{pmatrix}n & 1\end{pmatrix}$. And we have already shown that these in turn can be expressed as products of $\begin{pmatrix}1 & 2 & 3 & \cdots & n\end{pmatrix}$ and $\begin{pmatrix}1 & 2\end{pmatrix}$. The proof follows plainly.