Solution to Algebra I- MS- 14.pdf

(1) Consider the equivalence relation on $\mathbb{R}^2$ given by $(a_1, b_1) \equiv (a_2, b_2)$ iff $b_1 - a_1 = b_2 - a_2$. The equivalence classes of this relation are the family of lines $y = x + c$ for $c \in \mathbb{R}$.

(2) Given $m, n \in \mathbb{N}$ and $d = \gcd(m, n)$. Then $d = am + bn$ for some $a, b \in \mathbb{Z}$. Let q be any other common divisor of m and n. Then q divides $am + bn$, this implies q divides d.

(3) Clearly, $e \in G$ and for any $x \in G$, $x^{-1} \in G$. We only need to check that the aforementioned elements are respectively the identity and the inverse under the new operation $\circledcirc$. We have $x \circledcirc e = e \bullet x = x = x \bullet e = e \circledcirc x$ for $x \in G$ and $x \circledcirc x^{-1} = x^{-1} \bullet x = e = x \bullet x^{-1} = x^{-1} \circledcirc x$.

(4) Suppose $d|n$ and let $C_n =< a >$ then, $a^{n/d} \in C_n$ is an element of order exactly d. The subgroup $H =< a^{n/d} >$ is a subgroup of G of order d. Let K be any other subgroup of order d. Clearly, $K =< a^k >$ for some k dividing n. This implies that $d = |K| = o(a^k) = n/k$. Thus, $k = n/d$ and $K = H$. This proves uniqueness.

(5) G acts on itself by inner conjugation. For any $g \in G$, the element gg_0g^{-1} has order 2 as g_0 has order 2 for, $(gg_0g^{-1})^2 = gg_0^2g^{-1} = e$. Since g_0 is an unique element of order 2, one has $gg_0g^{-1} = g_0$ for every $g \in G$.

(6) Cauchy's theorem states that if G is a finite group and p is a prime dividing order of G then, G has an element of order p. As 2 and 3 are primes dividing 6, there exists elements of order 2, 3 in a group G of order 6.

(7) A *cycle* of length l in S_n is 1-1 onto mapping on $\{1, ..., n\}$ such that it maps a subset S of $\{1, ..., , n\}$ containing exactly l distinct elements $\{a_0, ..., a_{l-1}\}$ onto itself and fixes all elements outside S. Such a cycle is notated $(a_0, ..., a_{l-1})$. Let $\sigma = (a_0, ..., a_{l-1})$ be an l-cycle and let k be its order. If $0 < k < l$, then $\sigma^k(a_0) = a_k$, But $a_0 \neq a_k$ and so $\sigma^k \neq 1$. This implies $k \geqslant n$. Further, $\sigma^k(a_j) = a_{j+k(mod\ l)}$ implies σ^l is identity. As σ fixes all elements outside $\{a_0, ..., a_{l-1}\}$, σ^n also fixes those elements. Hence, from the above observations and as order of a permutation σ is the smallest positive integer n such that $\sigma^n = 1$, we conclude that order of σ is l. Now, let σ be any permutation in S_n. Let $\alpha \in \{1, ..., n\}$ and $C_\alpha = (\alpha, \sigma\alpha, \sigma^2\alpha, ..., \sigma^k\alpha)$ be orbit of α where k is such that $sigma^k\alpha = \alpha$. Clearly, C_α is a k-cycle. Next choose $\beta \in \{1, ..., n\}$ such that $\beta \notin C_\alpha$. Let $C_\beta = \{\beta, \sigma\beta, \sigma^2\beta, ..., \sigma^l\beta\}$ be the orbit of β with $\sigma^l\beta = \beta$. As before C_l is an l-cycle disjoint from C_α. Continue this process to obtain $\sigma = C_\alpha C\beta ... C_\gamma$. This process terminates as the set $\{1, ..., n\}$

is finite and as σ is an arbitrary permutation of S_n, one concludes that every permutation of S_n can be written as product of disjoint cycles.

(8) By Cauchy's theorem if a prime p divides order of a finite group G then G has an element a of order p. One has $< a >$ is a subgroup of G. By Lagrange's theorem the order of a subgroup divides the order of a group. Thus, if $|G| = p$ then $| < a > | = p$ if a is nonidentity element. Hence, upto isomorphism there exists an unique cyclic group of order 2, 3 and 5. Clearly, $G = \{e\}$ is the unique group of order 1. Coming to groups of order $4 = 2^2$, we assert that every group G of order 4 is abelian. In fact, suppose G is not abelian, then there exists non identity elements $a, b \in G$ such that $ab \neq ba$. Clearly, $b \neq a^{-1}$ so that $ab \neq 1 \neq ba$. Also, $ab \neq a \neq ba$ for otherwise $b = e$. Similarly, $ab \neq b \neq ba$. This gives 5 distinct elements e, a, b, ab, ba in the group G of order 4 which is a contradiction. Now, each nonidentity element of G has order 2 or 4. If $a \neq e$ has order 4 then $G =< a >$ is the cyclic group of order 4. If $a \neq e$ has order 2 then $H =< a >$ is a subgroup of G of order 2. Let $b \in G$ be such that $b \notin H$, *i.e.*, $b \neq e$. As $o(b)$ divides 4 and b cannot have order 4 (because then G will end up having more than 4 elements), we conclude $o(b) = 2$. Further, the third nonidentity element, say c, also has order 2. We assert that $c = ab$. If $ab = e$ then $b = a^{-1}$ contradicts $b = b^{-1}$. If $ab = a$ then $b = e$ and if $ab = b$ then $a = e$ contradicts the assumtion that a, b are nonidentity elements. Thus $ab = c = ba$. Arguing as above, we have $bc = a = cb$ and $ac = b = ca$. This gives the Klein-4-group $\{e, a, b, c\}$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ under the mapping $f : G \longmapsto \mathbb{Z}_2 \times \mathbb{Z}_2$ with $f(e) = (0, 0), f(a) = (1, 0), f(b) = (0, 1)$ and $f(c) = (1, 1)$.