Soham Chatterjee
Email: soham.chatterjee@tifr.res.in
Course: Mathematical Foundations for Computer Sciences

Assignment - 5
Dept: STCS
November 26, 2024

Problem 1

Solve the following parts.

- Prove that a group has exactly three subgroups if and only if it is cyclic of order p^2 for some prime p.
- Let $p < q$ be primes. Show that every group of order pq has a normal Sylow subgroup. Additionally, if p does not divide $q - 1$, then every such group is cyclic.

Solution:

- Suppose G has exactly 3 subgroups. Then G has only one proper subgroup. Let the proper subgroup is H. Then take $g \in G \setminus H$. Now $g \neq e$ where e is the identity element. Hence $\langle g \rangle = G$. Therefore G is cycle. Now G has 3 subgroups. Let $|G| = n$. Therefore n as exactly 3 divisors. Now if $d \mid n$ the then the number of order d elements in G is $\phi(d)$ where $\phi(d)$ is the Euler Totient function.

  Lemma 1. *The number of subgroups of a cyclic group G is the same as number of divisors of n where $|G| = n$.*

  Proof: Let $d \mid n$. Then there are $\phi(d)$ many elements of G whose order is d. Therefore take $h \in G$ such that order of h is d. Then take the subgroup $\langle h \rangle$. Clearly $|\langle h \rangle| = d$. Now for all h^k where $gcd(k, d) = 1$ and $k < d$ order of h^k is d. There are $\phi(d)$ many such k's. Hence all the elements in G of order d are in the subgroup $\langle h \rangle$. Therefore for each divisor there exists one subgroup of order d. Now if K is a subgroup of G. Then $|K| \mid n$. So each subgroup corresponds to a divisor of n. Therefore the number of subgroups of G and the number of divisors of n are same. □

  Since G has exactly 3 subgroups, n has exactly 3 divisors. And the numbers which have exactly 3 divisors are of the form p^2 for some prime p. Hence G has order p^2.

  Now let G is cyclic and G has order p^2. Now we just proved that number of divisors of n and the number of subgroups of a cyclic group are same. Since G has order p^2 and p^2 has 3 divisors, G has exactly 3 subgroups.

- Let G be the group with order pq. By Sylow Theorem there exists a $q-$Sylow subgroup. Let n_q denote the number of $q-$Sylow subgroups. Then we have

  $$n_q \equiv 1 \bmod q \qquad n_q \mid p$$

  Now the divisors of pq are $1, p, q, pq$. Among these $q \equiv 0 \bmod q$ and $pq \equiv 0 \bmod q$. Since $p < q$ we have $p \equiv p \bmod q$. Therefore the only possible value for $n_q = 1$. Hence there is an unique $q-$Sylow subgroup. Call it Q

  Lemma 2. *If a finite group G has only one subgroup of a given order then that subgroup is normal*

  Proof: Let H be a subgroup of G of given order. Let $g \in G$. Then gHg^{-1} is a subgroup of G. Now $|gHg^{-1}| = |H|$. Since there is exactly one subgroup of G of given order we have $gHg^{-1} = H$. Since this is true for any arbitrary g we have H is a normal subgroup. □

  Since here there is an unique $q-$Sylow subgroup it is normal by the lemma.

Now let n_p be the number of $p-$Sylow subgroups. Then $n_p \mid q$ and $n_p \equiv 1 \bmod p$. Therefore $n_p \in \{1, q\}$. We know $p \nmid q-1$. Therefore $n_p = 1$. Hence there is unique $p-$Sylow Subgroup. Call it P. Now the only common element of P and Q is the identity element e. Therefore $|P \cup Q| = p+q-1$. And $|G| = pq \geq 2q > q+p-1$. Hence $G \setminus (P \cup Q) \neq \emptyset$. Let $g \in G \setminus (P \cup Q)$. Then order of g is neither p nor q since $g \notin P$, $g \notin Q$. But order of g divides $|G| = pq$. Hence order of g is pq. Therefore g generates the whole group G. Hence if $p \nmid q-1$ then every such group is cyclic.

■

[Me and Soumyadeep solved this together.]

Problem 2

There are 100 students that take a test and get a score in the set $\{0, 1, 2, \ldots, 100\}$. Each student i has a number d_i he dislikes and is happy if his score and the sum of all his friends' score is not d_i more than some multiple of 101. Show that there are scores such that every student is happy.

Solution: Let S_i denote the set of students who are friends of the student i. Let x_i be the number student i got. Now student i is happy iff

$$x_i + \sum_{j \in S_i} x_j \not\equiv d_i \bmod 101 \iff x_i \not\equiv d_i - \sum_{j \in S_i} x_j \bmod 101$$

Now let I_i is the indicator random variable if student i is happy. That is $I_i = 1$ if student i is happy and $I_i = 0$ otherwise. Then

$$\mathbb{P}[I_i = 1] = \mathbb{P}\left[x_i \not\equiv d_i - \sum_{j \in S_i} x_j \bmod 101\right] = \frac{100}{101}$$

Now

$$\mathbb{E}\left[\sum_{i=1}^{100} I_i\right] = \sum_{i=1}^{100} \mathbb{E}[I_i] = \sum_{i=1}^{100} \frac{100}{101} > 99$$

Hence $\mathbb{P}\left[\sum_{i=1}^{100} I_i = 100\right] > 0$. Therefore there exists scores such that every student is happy. ■

Problem 3

Let R be a principal ideal domain. Show that:

- Every proper ideal of R is a product of finitely many maximal ideals, which are uniquely determined up to order.
- An ideal P of R is said to be primary if for all $a, b \in R$ such that $ab \in P$ and $a \notin P$, there exists $m > 0$ such that $b^m \in P$. Show that P is primary iff $P = \langle p^m \rangle$ for some m and some p that is either prime or 0 .
- Let $P_1, \ldots, P_n$ be primary ideals such that $P_i = \langle p_i^{m_i} \rangle$ for primes p_i that are not associates. Show that the product of these ideals equals their intersection.
- Every proper ideal of R is an intersection of finitely many primary ideals, which are uniquely determined up to order.

Solution:

- R is a principal ideal domain. Hence R is also an unique factorization domain. Now let I is a proper ideal of R. Since R is a principal ideal domain $\exists\ x \in R$ such that $I = \langle x \rangle$. Now since R is also an unique factorization domain the element x can be written uniquely as a finite product of prime elements of R up to associates such that $x = p_1^{e_1} \cdots p_k^{e_k}$. Then we claim $\langle x \rangle = \langle p_1 \rangle^{e_1} \cdots \langle p_k \rangle^{e_k}$.

Lemma 3. *If p is a prime element in R then for any k, $\langle p^k\rangle = \langle p\rangle^k$*

Proof: Let $a \in \langle p^k\rangle$. Then $\exists\ r \in R$ such that $a = rp^k$. But then $rp \in \langle p\rangle$ and $p \in \langle p\rangle$ Therefore $rp^k \in \langle p\rangle^k$. Therefore $\langle p^k\rangle \subseteq \langle p\rangle^k$. Now let $b \in \langle p\rangle^k$. Then $\exists\ r_1, \ldots, r_k \in R$ such that $b = \prod_{i=1}^{k} r_i p = \left[\prod_{i=1}^{k} r_i\right] p^k$. Denote $r \coloneqq \prod_{i=1}^{k} r_i$. Then $b = rp^k$. Hence $b \in \langle p^k\rangle$. Therefore $\langle p\rangle^k \subseteq \langle p^k\rangle$. Hence we have $\langle p^k\rangle = \langle p\rangle^k$. □

Lemma 4. $\langle x\rangle = \langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle$

Proof: Let $a \in \langle x\rangle$. Then there exists $r \in R$ such that $a = rx$. Since $x = p_1^{e_1} \cdots p_k^{e_k}$ we have $a = rp_1^{e_1} \cdots p_k^{e_k}$. Therefore $rp_1^{e_1} \in \langle p_1^{e_1}\rangle$ and $p_i \in \langle p_i^{e_i}\rangle$ for all $i \in \{2, \ldots, k\}$. Therefore $a \in \langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle$. Hence $\langle x\rangle \subseteq \langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle$.

Now let $b \in \langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle$. Then there exists $r_1, \ldots, r_k \in R$ such that $b = \prod_{i=1}^{k}(r_i p_i^{e_i}) = \left[\prod_{i=1}^{k} r_i\right] \prod_{i=1}^{k} p_i^{e_i}$. Now denote $r \coloneqq \prod_{i=1}^{k} r_i$. Then $b = r\prod_{i=1}^{k} p_i^{e_i} = rx$. Therefore $b \in \langle x\rangle$. Hence $\langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle \subseteq \langle x\rangle$. Therefore $\langle x\rangle = \langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle$. □

Hence $\langle x\rangle = \langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle$. Now using Lemma 3 we have

$$\langle x\rangle = \langle p_1^{e_1}\rangle \cdots \langle p_k^{e_k}\rangle = \langle p_1\rangle^{e_1} \cdots \langle p_k\rangle^{e_k}$$

Therefore $\langle x\rangle$ is the product of finitely many prime ideals. Now we will show that prime ideals are maximal ideals in a principal ideal domain.

Lemma 5. *Every nonzero prime ideal in a principal ideal domain is maximal ideal.*

Proof: Let $\langle p\rangle$ be a nonzero prime ideal in the principal ideal domain. Let $I = \langle y\rangle$ where $y \in R$ be any idea which contains $\langle p\rangle$. We will show that $I = \langle p\rangle$ or $I = R$. Since $\langle p\rangle \subseteq I$ we have $p \in I$. Therefore there exists $r \in R$ such that $p = ry$. Since $\langle p\rangle$ is a prime ideal and $ry \in \langle p\rangle$ either $r \in \langle p\rangle$ or $y \in \langle p\rangle$. If $y \in \langle p\rangle$ then $\langle y\rangle = \langle p\rangle$.. But if $r \in \langle p\rangle$ then $\exists\ s \in R$ such that $r = ps$. Then $p = ry = psy \implies sx = 1$. Therefore y is an unit. Therefore $I = R$. Hence $\langle p\rangle$ is a maximal ideal □

Since $\langle x\rangle = \langle p_1\rangle^{e_1} \cdots \langle p_k\rangle^{e_k}$, $\forall\ i \in [k]$, $\langle p_i\rangle$ is a maximal ideal. Therefore $\langle x\rangle$ can be written as a finitely many product of maximal ideals which are uniquely determined up to order.

- Suppose P is nonzero ideal. Since R is a principal ideal domain it is also an unique factorization domain. Since P is an ideal of R let P is generated by $x \in R$. Therefore the element x can be written uniquely as a finite product of prime elements of R up to associates such that $x = p_1^{e_1} \cdots p_k^{e_k}$. Let $x_i \coloneqq \prod_{j=i}^{n} p_j^{e_j}$.

  Let P is primary ideal. Then we have $x = p_1^{e_1} x_2$. So if $p_1^{e_1} \notin P$ then $x_2^{m_2} \in P$ for some $m_2 \in \mathbb{N}$, $m_2 > 0$. If $p_1^{e_1} \in P$ then $P = \langle p_1^{e_1}\rangle$ and we are done otherwise $x_2^{m_2} \in P$. Now $x_2^{m_2} = \prod_{j=2}^{n} p_j^{e_j m_2}$. Since $x_2^{m_2} \in P$ we have $x_2^{m_2} = xr$ for some $r \in R$. Now

$$x_2^{m_2} = xr \implies \prod_{j=2}^{n} p_j^{e_j m_2} = r\prod_{j=1}^{n} p_j^{e_j} \implies \prod_{j=2}^{n} p_j^{(m_2-1)e_j} = rp_1^{e_1} \implies p_1^{e_1} \mid \prod_{j=1}^{n} p_i^{(m_2-1)e_i}$$

Therefore $\exists\ i \in \{2, \ldots, k\}$ such that $p_1 \mid p_i^{(m_2-1)e_i}$. So p_1 and p_i are associates which is not possible unless $m_2 = 1$ or $P = 0$. Hence $m_2 = 1$. Therefore $x_2 \in P$.

Now suppose $x_i \in P$ for any $i \in \{2, \ldots, k\}$. Then $x_i = p_i^{e_i} x_{i+1}$. Therefore is $p_i^{e_i} \notin P$ then $x_{i+1}^{m_{i+1}} \in P$ for some $m_{i+1} \in \mathbb{N}$ and $m_{i+1} > 0$. If $p_i^{e_i} \in P$ then $P = \langle p_i^{e_i} \rangle$ and we are done. Else $x_{i+1}^{m_{i+1}} \in P$. Now

$$x_{i+1}^{m_{i+1}} = \prod_{j=i+1}^{k} p_j^{e_j m_{i+1}}$$

Since $x_{i+1}^{m_{i+1}} \in P$, $\exists\ r_{i+1} \in R$ such that $x_{i+1}^{m_{i+1}} = r_{i+1} \prod_{j=1}^{n} p_j^{e_j}$. Then we have

$$\prod_{j=i+1}^{k} p_j^{e_j m_{i+1}} = r_{i+1} \prod_{j=1}^{n} p_j^{e_j} \implies \prod_{j=i+1}^{k} p_j^{(m_{i+1}-1)e_j} = r \prod_{j=1}^{i} p_j^{e_j} \implies p_j \mid \prod_{j=i+1}^{k} p_j^{(m_{i+1}-1)e_j}\ \forall\ j \in [i]$$

Therefore for all $j \in [i]$, $\exists\ j_l \in \{i+1, \ldots, k\}$ such that

$$p_j \mid p_{j_l}^{(m_{i+1}-1)e_{j_l}}$$

Therefore p_j and p_{j_l} are associates which is not possible unless $m_{i+1} = 1$ or $P = 0$. Therefore $m_{i+1} = 1$. Hence $x_{i+1} \in P$.

Therefore we can continue like this and obtain either $p_1^{e_1} \in P \implies P = \langle p_1^{e_1} \rangle$ or else $p_1^{e_1} \notin P \implies x_2 \in P$. For second case either then $p_2^{e_2} \in P \implies P = \langle p_2^{e_2} \rangle$ or else $p_2^{e_2} \notin P \implies x_3 \in P$. For second case then $p_3^{e_3} \in P \implies P = \langle p_3^{e_3} \rangle$ or else $p_3^{e_3} \notin P \implies x_4 \in P$. Continuing like this we have if $x_i \in P$ then either $p_i^{e_i} \in P \implies P = \langle p_i^{e_i} \rangle$ or $p_i^{e_i} \notin P \implies x_{i+1} \in P$. And at the end we get either $p_{k-1}^{e_{k-1}} \in P \implies P = \langle p_{k-1}^{e_{k-1}}$ else $p_{k-1}^{e_{k-1}} \notin P \implies x_k = p_k^{e_k} \in P \implies P = \langle p_k^{e_k} \rangle$. Therefore we obtain $\exists\ i \in [k]$ such that $P = \langle p_i^{e_i} \rangle$.

Now suppose $P = \langle p^m \rangle$. Now let $ab \in P$ where $a, b \in R$. Suppose $a \notin P$. Since $ab \in P$, $p^m \mid ab \implies p \mid ab$. Since p is prime $p \mid a$ or $p \mid b$. Now we will show that if $b^k \notin P$ for all $K \in \mathbb{N}$ then $a \in P$. Now $b^k \notin P$ for all $k \in \mathbb{N}$. Hence $p^m \nmid b^k$ for all $k \in \mathbb{N}$. Therefore $p \nmid b$ since otherwise $p^n \mid b^n$. Therefore $p \mid a$. Since $p^n \mid ab$ and $p^n \nmid b$ we have $p^n \mid a$. Therefore $a \in P$. Hence P is primary ideal.

- Let $a \in \prod_{i=1}^{n} \langle p_i^{m_i} \rangle$. Then $\exists\ r_i \in R$ for all $i \in [n]$ such that

$$a = \prod_{i=1}^{n} r_i p_i^{m_i} = \underbrace{\left[\prod_{i=1}^{n} r_i\right]}_{r} \prod_{i=1}^{n} p_i^{m_i} = r \prod_{i=1}^{n} p_i^{m_i}$$

Now $r \in R$. And $r \prod_{i=1}^{n} p_i^{m_i} = \left[r \prod_{i \neq j} p_i^{m_i}\right] p_j^{m_j} \in \langle p_j^{m_j} \rangle$ for all $j \in [n]$. Hence $r \prod_{i=1}^{n} p_i^{m_i} \in \langle p_j^{m_j} \rangle$ for all $j \in [n]$. Therefore $r \prod_{i=1}^{n} p_i^{m_i} \in \bigcap_{i=1}^{n} \langle p_i^{m_i} \rangle$. Hence $\prod_{i=1}^{n} \langle p_i^{r_i} \rangle \subseteq \bigcap_{i=1}^{n} \langle p_i^{m_i} \rangle$.

Let $a \in \bigcap_{i=1}^{n} \langle p_i^{m_i} \rangle$. Then $\exists\ r_i \in R$ such that $a = r_i p_i^{m_i}$. Now

$$r_1 p_1^{m_1} = r_2 p_2^{m_2} \implies p_1 \mid r_2 p_2^{m_2}, p_2 \mid r_1 p_1^{m_1} \implies p_1 \mid p_2 \text{ or } p_1 \mid r_2 \text{ and } p_2 \mid p_1 \text{ or } p_2 \mid r_1$$

Since p_1 and p_2 are not associates we have $p_1 \mid r_2$ and $p_2 \mid r_1$. Since $p_1 \nmid p_2$ and $p_2 \nmid p_1$ we have $p_1^{m_1} \mid r_2$ and $p_2^{m_2} \mid r_1$. So let $r_1 = p_2^{m_2} r_1^{(2)}$ where $r^{(1)} \in R$. Then $a = p_1^{m_1} p_2^{m_2} r_1^{(2)}$. Now suppose we have $a = r_1^{(i)} \prod_{j=1}^{i} p_j^{m_j}$ where $r_1^{(i)} \in R$. Now $a = p_{i+1}^{m_{i+1}} r_{i+1}$. Therefore

$$r_1^{(i)} \prod_{j=1}^{i} p_j^{m_j} = p_{i+1}^{m_{i+1}} r_{i+1} \implies p_{i+1}^{m_{i+1}} \mid r_1^{(i)} \prod_{j=1}^{i} p_j^{m_j} \implies p_{i+1} \mid r_1^{(i)} \text{ or } \exists\ j \in [i],\ p_{i+1} \mid p_j^{m_j}$$

But p_{i+1} and p_j for all $j \in [i]$ are not associates. Therefore $p_{i+1} \nmid p_j^{m_j}$ for all $j \in [i]$. Hence $p_{i+1} \mid r_1^{(i)}$. Therefore $p_{i+1}^{m_{i+1}} \mid r_1^{(i)}$. Hence suppose $r_1^{(i)} = p_{i+1}^{m_{i+1}} r_1^{(i+1)}$ where $r_1^{(i+1)} \in R$. Therefore $a = r_1^{(i+1)} \prod_{j=1}^{i+1} p_j^{m_j}$. Therefore for $i = n$ we get $a = r_1^{(n)} \prod_{j=1}^{n} p_j^{m_j}$. Denote $r \coloneqq r_1^{(n)}$. Then $a = r \prod_{i=1}^{n} p_i^{m_i}$. Now $rp_1^{m_1} \in \langle p_1^{m_1}$ and for all $i \in \{2, \ldots, n\}$ we have $p_i^{m_i} \in \langle p_i^{m_i} \rangle$. Therefore $a = r_1^{(n)} \prod_{j=1}^{n} p_j^{m_j} \in \prod_{i=1}^{n} \langle p_i^{m_i} \rangle$. Hence $\bigcap_{i=1}^{n} \langle p_i^{m_i} \rangle \subseteq \prod_{i=1}^{n} \langle p_i^{m_i} \rangle$. Therefore we have $\bigcap_{i=1}^{n} \langle p_i^{m_i} \rangle = \prod_{i=1}^{n} \langle p_i^{m_i} \rangle$

- R is a principal ideal domain. Hence R is also an unique factorization domain. Now let I is a proper ideal of R. Since R is a principal ideal domain $\exists\ x \in R$ such that $I = \langle x \rangle$. Now since R is also an unique factorization domain the element x can be written uniquely as a finite product of prime elements of R up to associates such that $x = p_1^{e_1} \cdots p_k^{e_k}$. Hence by Lemma 4 we have $\langle x \rangle = \prod_{i=1}^{k} \langle p_i^{e_i} \rangle$. Now by te second part for all $i \in [k]$, $\langle p_i^{e_i} \rangle$ are primary ideals. Now by the last part we know $\prod_{i=1}^{k} \langle p_i^{e_i} \rangle = \bigcap_{i=1}^{k} \langle p_i^{e_i} \rangle$. Therefore we have $I = \langle x \rangle = \bigcap_{i=1}^{k} \langle p_i^{e_i} \rangle$. Hence every proper ideal of R is an intersection of finitely many primary ideals, which are uniquely determined up to order.

■

[Me and Soumyadeep solved this together.]

Problem 4

Shuffles and permutations.

- Show that two permutations π and σ are conjugates if and only if they have the same cycle structure, i.e., for all i, both π and σ have the same number of cycles of length i.
- Find the smallest $m > 1$ for which there are two cyclic permutations $\pi, \sigma \in S_m$ such that $\pi \circ \sigma \circ \pi^{-1} \circ \sigma^{-1}$ is a cyclic permutation.
- The riffle shuffle on a standard deck of playing cards is the shuffle where one partitions the cards into a top half and a bottom half, and, starting from the lowest card in the top half, interleaves cards from the two halves. Show that the riffle shuffle is not complete, i.e. there is no distribution $\mathcal{D}$ on $\mathbb{N}$ such that sampling a number n from $\mathcal{D}$ and performing n riffle shuffles starting from a perfectly ordered deck of cards yields a uniformly random deck of cards.

  More generally, a set of k shuffles is said to be complete if there is a distribution $\mathcal{D}$ over finite strings with alphabet $[k]$ such that sampling a string s from $\mathcal{D}$ and performing shuffles $s_1, s_2, \ldots$ (in order) starting from a perfectly ordered deck of cards yields a uniformly random deck of cards. What is the size of the smallest complete set of shuffles that contains the riffle shuffle?

Solution:

- Let π and σ are conjugates. Then $\exists$ a permutation τ such that $\pi = \tau\sigma\tau^{-1}$. Suppose $\sigma(i) = j$. Then

$$\pi(\tau(i)) = \tau\sigma\tau^{-1}(\tau(i)) = \tau\sigma(i) = \tau(j)$$

Therefore if $i_1 \to i_2 \to \ldots, i_k \to i_1$ is a k length cycle in σ. Then $\tau(i_1) \to \tau(i_2) \to \cdots \to \tau(i_k) \to \tau(i_1)$ is also cycle in π. So each k length cycle in σ corresponds to a k length cycle in π for all k. Therefore π and σ has the same cycle structure.

Let π and σ have same cycle structure. Let $i_1 \to i_2 \emptyset \cdots i_k \to i_1$ be a k length cycle in σ and $j_1 \to j_2 \emptyset \cdots j_k \to j_1$ be a k length cycle in π. Then let τ be the permutation such that $\tau(i_l) = j_l$ for each $l \in [k]$. Then

$$\tau\sigma\tau^{-1}(j_l) = \tau\sigma(i_l) = \tau(i_{l+1}) = j_{l+1} \quad \text{where by } ik+1, j_{k+1} \text{ we mean } i_1, j_1$$

We do this for all k length cycles in σ and π for all k. Therefore we get a permutation τ such that $\pi = \tau\sigma\tau^{-1}$. Hence π and τ are conjugates.

- For any two permutations σ, π we call $\sigma \circ \pi \circ \sigma^{-1} \circ \pi^{-1}$ as the commutator of σ and π and denote by $[\sigma, \pi]$. $m = 2$ is not possible since $S_2 = \{id, (12)\}$ where id is not a cyclic permutation. $(12)(12) = id$. Therefore $m > 3$. Now for $m = 3$ we have only two 3 length cycles which are (123) and (132) and $(123)^{-1} = (132)$. So we can not take $\pi = (123)$ and $\sigma = (132)$ since $\pi\sigma\pi^{-1}\sigma^{-1} = id$. So $\pi = \sigma$. In that case we have $(123)(123) = (132)$ and $(132)(132) = (123)$. So

$$(123)(123)(132)(132) = id \qquad (132)(132)(123)(123) = id$$

So in case of S_3 this is not possible. Now for S_4 we have calculated all possible commutators of all 6 4−length cycles in S_4 with the following python code:

```
from sympy.combinatorics import Permutation, PermutationGroup
# We have taken (0,1,2,3) instead of (1,2,3,4) to make the code work
cycle_1 = Permutation([1, 2, 3, 0])  # (0 1 2 3)
cycle_2 = Permutation([1, 3, 0, 2])  # (0 1 3 2)
cycle_3 = Permutation([2, 3, 1, 0])  # (0 2 1 3)
cycle_4 = Permutation([2, 0, 3, 1])  # (0 2 3 1)
cycle_5 = Permutation([3, 2, 0, 1])  # (0 3 1 2)
cycle_6 = Permutation([3, 0, 1, 2])  # (0 3 2 1)

six_cycles = [cycle_1, cycle_2, cycle_3, cycle_4, cycle_5, cycle_6]

# Function to compute the commutator of two permutations
def commutator(p1, p2):
        return p1 * p2 * p1**-1 * p2**-1

# Compute all commutators of 4-cycles
for sigma in six_cycles:
        for tau in six_cycles:
                print(sigma, tau, commutator(sigma, tau))
```

And we got the following table:

$[(1234), (1234)] = id$	$[(1234), (1243)] = (143)$	$[(1234), (1324)] = (243)$
$[(1234), (1342)] = (132)$	$[(1234), (1423)] = (142)$	$[(1234), (1432)] = id$
$[(1243), (1234)] = (134)$	$[(1243), (1243)] = id$	$[(1243), (1324)] = (132)$
$[(1243), (1342)] = id$	$[(1243), (1423)] = (234)$	$[(1243), (1432)] = (142)$
$[(1324), (1234)] = (234)$	$[(1324), (1243)] = (123)$	$[(1324), (1324)] = id$
$[(1324), (1342)] = (142)$	$[(1324), (1423)] = id$	$[(1324), (1432)] = (143)$
$[(1342), (1234)] = (123)$	$[(1342), (1243)] = id$	$[(1342), (1324)] = (124)$
$[(1342), (1342)] = id$	$[(1342), (1423)] = (143)$	$[(1342), (1432)] = (243)$
$[(1423), (1234)] = (124)$	$[(1423), (1243)] = (243)$	$[(1423), (1324)] = id$
$[(1423), (1342)] = (134)$	$[(1423), (1423)] = id$	$[(1423), (1432)] = (132)$
$[(1432), (1234)] = id$	$[(1432), (1243)] = (124)$	$[(1432), (1324)] = (134)$
$[(1432), (1342)] = (234)$	$[(1432), (1423)] = (123)$	$[(1432), (1432)] = id$

Hence in case S_4 such two permutations are not possible. Now in S_5 take $\sigma = (12345)$ and $\pi = (13542)$. Then

$$\sigma^{-1} = (54321) = (15432) \qquad \pi^{-1} = (24531) = (12453)$$

Now we have

$$\sigma \circ \pi = (143) \qquad \sigma^{-1} \circ \pi^{-1} = (253)$$

Therefore

$$[\sigma, \pi] = \sigma \circ \pi \circ \sigma^{-1} \circ \pi^{-1} = (143)(253) = (14532)$$

Therefore the smallest m is 5.

[Me and Soumyadeep solved this together.]

Problem 5

Prove/disprove:

- If R is a ring with identity but without any proper right ideals, the R is a division ring.
- Let n be an integer and R be a ring such that $r^n = r$ for all $r \in R$. Then, the characteristic of R is square-free. Moreover, if n is even, R has characteristic 2 .
- The sum of two principal ideals is a principal ideal.

Solution:

- Let a be an element of R, $a \neq 0$. Now if $\langle a \rangle \subsetneq R$ then R has a proper ideal which is not possible. Hence $aR = R$. So $1 \in aR$. Therefore $\exists\ b \in R$ such that $ab = 1$. Now we also have $bR = R$. Therefore $\exists\ c \in R$ such that $bc = 1$. Then we have

  $$a = a(bc) = (ab)c = c$$

  So the multiplicative inverse of a exists in R and it is b. Therefore a is an unit. Since a is an arbitrary nonzero element in R, R is a division ring.

  So the statement is True.

- Let r be any element of R. Let m denotes the characteristic of R. Suppose m is not square free. Then there exists a prime p such that $p^2 \mid m$. Now we have $(pr)^n = pr$.

  Lemma 6. *$(pr)^n = p^n r^n$ for all positive integer n.*

  Proof: We will show this by induction. For $n = 1$ this is true. Hence the base case follows. Suppose this is true for $n - 1$. Then

  $$(pr)^n = (pr)^{n-1} \sum_{i=1}^{p} r = p^{n-1} r^{n-1} \sum_{i=1}^{p} r = \sum_{i=1}^{p} p^{n-1} r^n = p^n r^n$$

  □

  So now

  $$(pr)^n = p^n r^n = p^n r = pr \implies (p^n - p)r = 0$$

  Therefore $m \mid p^n - p$. Now $p^2 \mid m$. Therefore $p^2 \mid p^n - p$. Now $p^n - p = p(p^{n-1} - 1)$. Hence $p \mid p^{n-1} - 1$ but that is not possible. Hence m is square free.

  Now let p be a prime such that $p \mid m$. Let r be any element of R. Now $((p-1)r)^n = (p-1)r$ and we have $((p-1)r)^n = (p-1)^n r^n = (p-1)^n r$. Therefore $((p-1)^n - (p-1))r = 0$. Therefore $m \mid (p-1)^n - (p-1)$. Therefore $p \mid (p-1)^n - (p-1) \implies p \mid (p-1)((p-1)^{n-1} - 1) \implies p \mid (p-1)^{n-1} - 1 \implies (p-1)^{n-1} \equiv 1 \bmod p$. Now

  $$(p-1) \equiv -1 \bmod p \implies (p-1)^{n-1} \equiv (-1)^{n-1} \equiv -1 \bmod p \implies 1 \equiv -1 \bmod p \implies 2 \equiv 0 \bmod p$$

  Now $2 \equiv 0 \bmod p$ is only possible when $p = 2$. Therefore the only prime that divides p is 2. Hence $m = 2$. So the statement is True.

- In the ring $\mathbb{Z}[x]$ take the ideals $\langle 3 \rangle$ and $\langle x \rangle$. Now the sum of these two ideals contains both 3 and x and therefore $\langle 3 \rangle + \langle x \rangle = \langle 3, x \rangle$. Which is not a principal ideal domain.

  Hence this statement is false.

■

[Me and Soumyadeep solved this together.]