

For example, $x = (12) \in S_3$ has 3 conjugates $(12), (23), (13)$ and its centralizer $C((12)) = \{e, (12)\}$ has 2 elements and these two numbers give $2 \cdot 3 = 6 = |S_3|$.

Putting these together we get:

$$|G| = \sum_{i=1}^c |G \cdot x_i| = \sum_{i=1}^c |G : C(x_i)|$$

In the case of $G = S_3$ this is:

$$\begin{aligned} |S_3| &= |S_3 : C(e)| + |S_3 : C((12))| + |S_3 : C((123))| \\ 6 &= 1 + 3 + 2 \end{aligned}$$

The first number is 1 since $C(e) = S_3$.

Problem: a) Show that $C(g) = G$ if and only if $g \in Z(G)$.

b) Show that every element of $Z(G)$ is in its own conjugacy class.

This implies that the number of times the index $|G : C(x_i)|$ is equal to 1 is the number of elements in the center $Z(G)$. Call this $z = |Z(G)|$. For example, $z = |G|$ if G is abelian.

Theorem 17.3 (class formula). *If G is a finite group then*

$$|G| = |Z(G)| + \sum_{\neq 1} \underbrace{|G : C(x_i)|}$$

Corollary 17.4. *If the order of G is a power of a prime: $|G| = p^k, k \geq 1$ then G has a nontrivial center.*

Proof. In the class formula, all the numbers divide p^k . So, the numbers which are not 1, such as $|G|$ and $|G : C(x_i)|$ are multiples of p . Therefore, $|Z(G)|$ is divisible by p . But $e \in Z(G)$. So $Z(G)$ must have at least p elements. \square

For example D_4 has $8 = 2^3$ elements and its center has $p = 2$ elements.

Corollary 17.5. *There are no nonabelian simple p -groups (groups whose order is a power of the prime p).*

Proof. Any nontrivial p -group P has a nontrivial center $Z(P)$ which we know is a normal subgroup of P . If P is simple then we must have $P = Z(P)$. So, P is abelian (which implies P has order p . Why?) \square

18. RINGS AND FIELDS

Definition 18.1. A **ring** $(R, +, \cdot)$ is a set R with two binary operations: addition $+$ and multiplication \cdot so that

- (1) $(R, +)$ is an additive group.
- (2) Multiplication is associative.
- (3) Multiplication distributes over addition on both sides, i.e.:

$$a(x + y) = ax + ay$$

$$(x + y)b = xb + yb$$

Example 18.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings with the usual operations of addition and multiplication. We will assume that multiplication is associative and distributive over addition without proof for these common rings. These rings are all commutative rings.

Definition 18.3. A **commutative ring** is ring R in which the multiplication is commutative: $ab = ba$ for all $a, b \in R$. (Addition is always commutative.)

Example 18.4. $M_n(\mathbb{R})$ is the ring of all $n \times n$ matrices with coefficients in \mathbb{R} . This is a ring with matrix addition

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})_{ij}$$

and matrix multiplication:

$$(a_{ij})(b_{ij}) = \left(\sum_{j=1}^n a_{ij}b_{jk} \right)_{ik}$$

The notation is that $(xxx)_{ij}$ is the matrix whose ij entry is the thing written in xxx . A more precise, rigorous definition is: $AB = C$ where the entries of C in terms of the entries of A, B are:

$$c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$$

The ring $M_n(\mathbb{R})$ is not commutative for $n \geq 2$. For example:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Proposition 18.5. If R is any ring then $M_n(R)$, the set of $n \times n$ matrices with coefficients in R

But these rings all have unity.