Symmetries in Physics

Marco Biroli

September 4, 2020

Chapter 1

TD1

1.1 Problem 1 Cayley tables

1.1.1

Suppose that an element appears more than once in a given row or column. Then we have that:

$$\exists g, g_i, g_j, g_k \in \mathcal{G}, \quad g = g_i \cdot g_j \wedge g = g_i \cdot g_k \Rightarrow g_j = g_k$$

Since no two elements in a row can be mapped to the same element of the group then a row is a map $\mathcal{G} \to \mathcal{G}$ which from the point above is injective then since it is an endomorphism it necessarily must be a bijection and hence a permutation of $\mathcal{G}$. Therefore each element appears once and exactly once.

1.1.2

Refer above.

1.2 Problem 2 The group D_3

1.2.1

The elements of D_3 are $e = Id$, $r = (B, C, A)$, $r^2 = (C, A, B)$, $s_1 = (A, C, B)$, $s_2 = (B, A, C)$, $s_3 = (C, B, A)$. Then the table is given by:

	e	r	r^2	s_1	s_2	s_3
e	e	r	r^2	s_1	s_2	s_3
r	r	r^2	e	s_2	s_3	s_1
r^2	r^2	e	r	s_3	s_1	s_2
s_1	s_1	s_2	s_3	e	r	r^2
s_2	s_3	s_1	s_2	r^2	e	r
s_3	s_2	s_3	s_1	r	e	r^2

1.2.2

The subgroups of D_3 are $\{e, r, r^2\} = \langle r \rangle$, $\langle s_1 \rangle$, $\langle s_2 \rangle$, $\langle s_3 \rangle$, $\{e\}$.

1.3 Problem 3 Lagrange's theorem.

Let $\mathcal{H}$ be a subgroup of $\mathcal{G}$. Then notice that $\mathcal{G}/\mathcal{H}$ is the set of the cosets of $\mathcal{G}$ by the congruence modulo $\mathcal{H}$. However from Exercise 1 and 2 we know that every coset is in bijection with $\mathcal{H}$. Furthermore since the congruence is an equivalence relation it must be that $\mathcal{G}$ is equal to the reunion of the cosets. Hence we have that:

$$|\mathcal{G}/\mathcal{H}| \cdot |\mathcal{H}| = |\mathcal{G}|$$

The result follows.

1.4 Problem 4 Modular arithmetics

1.4.1

Notice that for any $k \in \mathbb{Z}$ we have that $k\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. The quotient groups are $\mathbb{Z}_{k\mathbb{Z}}$ which are the well-known integers modulo k with the addition modulo k.

1.4.2

Let $|g|$ be the smallest integer such that $g^{|g|} = e$. Such an integer must exist so long as the group to which g pertains is finite. Then notice that for any $k \in \mathbb{Z}$ we have that: $g^{|g| \cdot k} = (g^{|g|})^k = e^k = e$. Hence $|g|\mathbb{Z} \subseteq P_g$. Now let $k \in \mathbb{Z}$ such that $g^k = e$. From construction it must be that $k > |g|$ hence by doing the euclidean division we get that : $k = |g| \cdot \ell + r$. Hence: $g^{|g| \cdot \ell + r} = e \Rightarrow e^\ell \cdot g^r = e \Rightarrow g^r = e$. However unless $r = 0$ this is impossible since $r < |g|$ would be a contradiction.

1.4.3

Notice that necessarily $\langle g \rangle$ is a subgroup of cardinality $|g|$ of $\mathcal{G}$ hence from the Lagrange theorem we know that $|g|$ divides $|\mathcal{G}|$.

1.4.4

Let a group $\mathcal{G}$ of order p where p is prime. Then from the previous question we know that all elements of $\mathcal{G}$ must be of order p. However if one element is of order p and $\mathcal{G}$ is of order p it must be that $\mathcal{G}$ is generated by a single element, call it g. Then the obvious homomorphism concludes the proof:

$$\begin{aligned} h : \mathcal{G} &\to \mathbb{Z}/p\mathbb{Z} \\ g^k &\mapsto k \mod p \end{aligned}$$