Course 5

1.7 Equivalence relations induced by a subgroup

Definition 1.7.1 Let $(G, \cdot)$ be a group and let $H \leq G$. Define the homogeneous relations r_H and r'_H on G by

$$x \, r_H \, y \Longleftrightarrow x^{-1} \cdot y \in H \,,$$
$$x \, r'_H \, y \Longleftrightarrow y \cdot x^{-1} \in H \,.$$

Remark 1.7.2 (1) If the group G is commutative, then $r_H = r'_H$.

(2) Since $H \leq G$, the restriction of r_H (and r'_H) to H is clearly the universal relation on H.

Theorem 1.7.3 *Let $(G, \cdot)$ be a group and let $H \leq G$.*
(i) The relations r_H and r'_H previously defined are equivalence relations on G.
(ii)

$$G/r_H = \{xH \mid x \in G\} \,,$$
$$G/r'_H = \{Hx \mid x \in G\} \,,$$

where we denote $xH = \{x \cdot h \mid h \in H\}$ and $Hx = \{h \cdot x \mid h \in H\}$.

Proof. (i) We will prove that r_H is an equivalence relation on G, using several times the fact that $H \leq G$.

The relation r_H is reflexive, since $\forall x \in G$, $x^{-1} \cdot x = 1 \in H$, that is, $x \, r_H \, x$.

Let $x, y, z \in G$ be such that $x \, r_H \, y$ and $y \, r_H \, z$. Then $x^{-1} \cdot y \in H$ and $y^{-1} \cdot z \in H$, so that $x^{-1} \cdot z = x^{-1} \cdot y \cdot y^{-1} \cdot z \in H$. Hence $x \, r_H \, z$ and consequently r_H is transitive.

Let $x, y \in G$ be such that $x \, r_H \, y$. Hence $x^{-1} y \in H$. Then $y^{-1} \cdot x = (x^{-1} \cdot y)^{-1} \in H$. Thus, $y \, r_H \, x$ and consequently r_H is symmetric.

Hence r_H is an equivalence relation on G. Similarly, r'_H is an equivalence relation on G.

(ii) Since r_H and r'_H are equivalence relations on G, we know that $G/r_H = \{r_H < x > \mid x \in G\}$ and $G/r'_H = \{r_H < x > \mid x \in G\}$ are partitions of G. For every $x \in G$, we have

$$r_H < x > = \{y \in G \mid x \, r_H \, y\} = \{y \in G \mid x^{-1} \cdot y \in H\} = \{y \in G \mid y \in xH\} = xH.$$

Hence we have $G/r_H = \{xH \mid x \in G\}$. Similarly for G/r'_H. □

Definition 1.7.4 The relations r_H and r'_H are called the *(left and right) equivalence relations induced by the subgroup H of G.*

In general, the partitions G/r_H and G/r'_H do not coincide, but we have connections between them.

Definition 1.7.5 We say that two sets A and B *have the same cardinal*, and we denote it by $|A| = |B|$, if there exists a bijection between A and B.

Recall that by the cardinal of a finite set we simply understand the number of elements of that set.

Theorem 1.7.6 *Let $(G, \cdot)$ be a group and let $H \leq G$. Then:*
(i) $\forall x \in G$, $|xH| = |Hx| = |H|$.
(ii) $|G/r_H| = |G/r'_H|$.

Proof. (i) Let $x \in G$ and consider $\alpha : H \to xH$ defined by $\alpha(h) = x \cdot h$, $\forall h \in H$. It is easy to see that α is a bijection. Similarly, there is a bijection between H and Hx, and consequently between xH and Hx.

(ii) Define

$$f : G/r_H \to G/r'_H \text{ by } f(xH) = Hx^{-1} \,,\ \forall x \in G \,,$$
$$g : G/r'_H \to G/r_H \text{ by } g(Hx) = x^{-1}H \,,\ \forall x \in G \,.$$

Since H is a subgroup of G, the definitions of f and g are independent of the choice of representatives (that is, f and g are well-defined functions), because we have:

$$xH = yH \Longrightarrow (xH)^{-1} = (yH)^{-1} \Longrightarrow H^{-1}x^{-1} = H^{-1}y^{-1} \Longrightarrow Hx^{-1} = Hy^{-1} \,,$$

where we have denoted $X^{-1} = \{x^{-1} \mid x \in X\}$ for some set $X \subseteq G$.

Let us now prove that $g \circ f = 1_{G/r_H}$ and $f \circ g = 1_{G/r'_H}$. For every $x \in G$, we have

$$(g \circ f)(xH) = g(f(xH)) = g(Hx^{-1}) = (x^{-1})^{-1}H = xH\,,$$

$$(f \circ g)(Hx) = f(g(Hx)) = f(x^{-1}H) = H(x^{-1})^{-1} = Hx\,.$$

Hence f is a bijection. □

Definition 1.7.7 Let $(G, \cdot)$ be a group and let $H \leq G$. Then we denote

$$|G : H| = |G/r_H| = |G/r'_H|$$

and we call it the *index of H in G*.

Theorem 1.7.8 (Lagrange) *Let $(G, \cdot)$ be a finite group and let $H \leq G$. Then*

$$|G| = |G : H| \cdot |H|\,.$$

Proof. The equivalence classes xH $(x \in G)$ partition G into $|G : H|$ parts, each of which having exactly $|H|$ elements (see Theorem 1.7.6). □

Corollary 1.7.9 *Let $(G, \cdot)$ be a finite group. Then:*

(i) $\forall H \leq G$, $\operatorname{ord} H | \operatorname{ord} G$.

(ii) $\forall x \in G$, $\operatorname{ord} x | \operatorname{ord} G$.

(iii) $\forall x \in G$, $x^{|G|} = 1$.

(iv) If $|G| = p$ for some prime p, then G is cyclic and it is generated by any non-identity element.

Proof. (i) By the Lagrange Theorem.

(ii) Let $x \in G$ and use the Lagrange Theorem for $H = < x >$. Then $\operatorname{ord} x = | < x > |$ divides $\operatorname{ord} G$.

(iii) Consider the finite subgroup $< x >$ of G, say $| < x > | = k$. Then $\operatorname{ord} x = k$, and thus we have $x^k = 1$. But k divides $|G|$, hence $|G| = kd$ for some $d \in \mathbb{N}$. It follows that $x^{|G|} = (x^k)^d = 1$.

(iv) Let $x \in G$, $x \neq 1$. Then by the Lagrange Theorem, $\operatorname{ord} x | p$, so that $\operatorname{ord} x = p$, since $x \neq 1$. Hence $< x >$ is a subgroup of G having p elements. Therefore, $< x >= G$. □

Example 1.7.10 Consider the permutation group $(S_3, \circ)$ with $S_3 = \{e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, where

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Let $H = \{e, \sigma_1\}$ and $N = \{e, \sigma_4, \sigma_5\}$. By computing $\sigma \circ H$, $H \circ \sigma$, $\sigma \circ N$ and $N \circ \sigma$ for every $\sigma \in S_3$, we obtain

$$S_3/r_H = \{\sigma \circ H \mid \sigma \in S_3\} = \{\{e, \sigma_1\}, \{\sigma_2, \sigma_5\}, \{\sigma_3, \sigma_4\}\}\,,$$

$$S_3/r'_H = \{H \circ \sigma \mid \sigma \in S_3\} = \{\{e, \sigma_1\}, \{\sigma_2, \sigma_4\}, \{\sigma_3, \sigma_5\}\}\,,$$

$$S_3/r_N = \{\sigma \circ N \mid \sigma \in S_3\} = \{\{e, \sigma_4\, \sigma_5\}, \{\sigma_1, \sigma_2, \sigma_3\}\}\,,$$

$$S_3/r'_N = \{N \circ \sigma \mid \sigma \in S_3\} = \{\{e, \sigma_4\, \sigma_5\}, \{\sigma_1, \sigma_2, \sigma_3\}\}\,.$$

Note that all these must be partitions of G having the same number of elements (by the Lagrange Theorem). We have $S_3/r_H \neq S_3/r'_H$ and $S_3/r_N = S_3/r'_N$. Therefore, there exist non-commutative groups such that the left and the right equivalence relations induced by a subgroup coincide. We also have $|S_3 : H| = 3$ and $|S_3 : N| = 2$.

1.8 Normal subgroup. Factor group

We have seen that the equivalence relations induced by a subgroup coincide in the case of a commutative group, but not only in that situation. This is the motivation for introducing the following definition, that considers the subgroups H of a group G such that $r_H = r'_H$.

Definition 1.8.1 Let $(G, \cdot)$ be a group and let $N \leq G$. Then N is called a *normal subgroup* of G if $r_N = r'_N$. We denote by $N \trianglelefteq G$ the fact that N is a normal subgroup of G.

Theorem 1.8.2 *Let $(G, \cdot)$ be a group and let $N \leq G$. Then the following statements are equivalent:*
(i) $N \trianglelefteq G$;
(ii) $\forall x \in G$, $xN = Nx$;
(iii) $\forall x \in G$, $\forall n \in N$, $x^{-1} \cdot n \cdot x \in N$.

Proof. $(i) \Longleftrightarrow (ii)$ Since r_N and r'_N are equivalence relations on G, then by Theorem 1.7.3, we have:

$$r_N = r'_N \Longleftrightarrow r_N < x >= r'_N < x > , \forall x \in G \Longleftrightarrow xN = Nx \, , \forall x \in G \, .$$

$(ii) \Longrightarrow (iii)$ Assume that $\forall x \in G$, $xN = Nx$. Then $\forall x \in G$ we have:

$$xN = Nx \Longleftrightarrow N = x^{-1}Nx \Longrightarrow x^{-1}Nx \subseteq N \Longrightarrow \forall n \in N, x^{-1} \cdot n \cdot x \in N.$$

$(iii) \Longrightarrow (ii)$ Assume that $\forall x \in G$, $\forall n \in N$, $x^{-1} \cdot n \cdot x \in N$. Then $\forall x \in G$ we have:

$$\forall n \in N, x^{-1} \cdot n \cdot x \in N \Longrightarrow \forall n \in N, n \cdot x \in xN \Longrightarrow Nx \subseteq xN.$$

Using the hypothesis for x^{-1} for every $x \in G$, we have:

$$\forall n \in N, (x^{-1})^{-1} \cdot n \cdot x \in N \Longrightarrow \forall n \in N, x \cdot n \cdot x^{-1} \in N \Longrightarrow \forall n \in N, x \cdot n \in Nx \Longrightarrow xN \subseteq Nx.$$

Hence $xN = Nx$. □

Example 1.8.3 (a) Let $(G, \cdot)$ be a group. Then the trivial subgroups $\{1\}$ and G are clearly normal subgroups. A group that has only trivial normal subgroups is called *simple*.

(b) Every subgroup of a commutative group is normal.
As a consequence, the normal subgroups of $(\mathbb{Z}, +)$ are all its subgroups, namely $\{n\mathbb{Z} \mid n \in \mathbb{N}\}$.

(c) The subgroup H in Example 1.7.10 is not normal in S_3, whereas N in the same example is a normal subgroup of S_3.

Corollary 1.8.4 *Every subgroup of index 2 of a group is normal.*

Proof. Let $(G, \cdot)$ be a group and let $H \leq G$ be such that $|G : H| = 2$. Then $|G/r_H| = |G/r'_H| = |G : H| = 2$. By Theorem 1.7.3 we have $G/r_H = \{H, xH\}$ and $G/r'_H = \{H, Hx\}$ for any $x \in G \setminus H$. But G/r_H and G/r'_H are partitions of G, so that we must have $xH = G \setminus H = Hx$ for every $x \in G \setminus H$. Hence $H \trianglelefteq G$ by Theorem 1.8.2. □

Definition 1.8.5 Let $(G, \cdot)$ be a group and let $N \trianglelefteq G$. Then we denote

$$G/r_N = G/r'_N = \{xN \mid x \in G\}$$

by G/N and define on G/N an operation " $\cdot$ " by

$$(xN) \cdot (yN) = (x \cdot y)N \, , \quad \forall x, y \in G \, .$$

Theorem 1.8.6 *In the context of the previous definition, $(G/N, \cdot)$ is a group, called the quotient (factor) group of G modulo N.*

Proof. Let us prove first that the definition of the operation in G/N does not depend on the choice of representatives. Indeed, if $xN = x'N$ and $yN = y'N$, then $xyN = xy'N = xNy' = x'Ny' = x'y'N$.

The associative law in G/N follows easily by the associative law in G. The identity element in G/N is $1 \cdot N = N$ and $\forall x \in G$, we have $(xN)^{-1} = x^{-1}N$. Hence $(G/N, \cdot)$ is a group. □

Corollary 1.8.7 *Let $(G,\cdot)$ be a group and let $N \trianglelefteq G$. Then the natural projection $p_N : G \to G/N$, defined by $p_N(x) = xN$, $\forall x \in G$, is a surjective group homomorphism and* $\operatorname{Ker} p_N = N$.

Proof. The map p_N is a group homomorphism, since $p_N(xy) = (xy)N = (xN)(yN) = p_N(x)p_N(y)$, $\forall x, y \in G$. Clearly, p_N is surjective and $\operatorname{Ker} p_N = \{x \in G \mid p_N(x) = N\} = \{x \in G \mid xN = N\} = N$. $\square$

Theorem 1.8.8 (Correspondence Theorem) *Let $(G,\cdot)$ be a group and let $N \trianglelefteq G$. Then there is a bijective correspondence $\alpha : \{H \leq G \mid N \subseteq H\} \to S(G/N)$, $\alpha(H) = H/N$ with inverse $\beta : S(G/N) \to \{H \leq G \mid N \subseteq H\}$, $\beta(H') = \{x \in G \mid xN \in H'\}$.*

Proof. Let us show that α is well-defined. For $H \leq G$ we prove that $H/N \leq G/N$. We have $1 \in H$, hence $N = 1 \cdot N \in G/N$. For every $xN, yN \in H/N$ we have

$$(xN) \cdot (yN)^{-1} = (xN) \cdot (y^{-1}N) = (xy^{-1})N \in H/N.$$

Let us show that β is well-defined. For $H' \leq G/N$ we prove that $N \subseteq B = \{x \in G \mid xN \in H'\} \leq G$. We have $N \subseteq B$, because $n \in N \Longrightarrow nN = N \in H' \Longrightarrow n \in B$. Also, clearly $1 \in B$. For every $x, y \in B$ we have $xN, yN \in H'$, hence $xN, (yN)^{-1} \in H'$. Then

$$(xy^{-1})N = (xN) \cdot (y^{-1}N) = (xN) \cdot (yN)^{-1} \in H',$$

and so $xy^{-1} \in B$. Thus $B \leq G$.

For every $H \leq G$ with $N \subseteq H$ and $H' \leq G/N$ we have:

$$\beta(\alpha(H)) = \beta(H/N) = \{x \in G \mid xN \in H/N\} = H,$$

$$\alpha(\beta(H')) = \alpha(\{x \in G \mid xN \in H'\}) = \{xN \mid xN \in H'\} = H'.$$

Hence α and β are inverse to each other. $\square$

Example 1.8.9 Consider the group $(\mathbb{Z}_4, +)$. We may see $\mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\} = \{x + 4\mathbb{Z} \mid x \in \mathbb{Z}\} = \mathbb{Z}/4\mathbb{Z}$. Then the subgroups of $\mathbb{Z}_4$ are of the form $H/4\mathbb{Z}$ with $4\mathbb{Z} \subseteq H \leq \mathbb{Z}$. Then $4\mathbb{Z} \subseteq H = n\mathbb{Z}$, hence $n|4$, and so $n \in \{1, 2, 4\}$. Therefore, the subgroups of $\mathbb{Z}_4$ are: $1\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}_4$, $2\mathbb{Z}/4\mathbb{Z} = \{2x + 4\mathbb{Z} \mid x \in \mathbb{Z}\} = \{\widehat{0}, \widehat{2}\}$ and $4\mathbb{Z}/4\mathbb{Z} = \{\widehat{0}\}$.

One may immediately draw the Hasse diagram of the subgroup lattice of $(\mathbb{Z}_4, +)$.

Consider $N = \{\widehat{0}, \widehat{2}\}$. By Lagrange's Theorem it follows that $|\mathbb{Z}_4/N| = |\mathbb{Z}_4|/|N| = 2$. We have:

$$\mathbb{Z}_4/N = \{\widehat{x} + N \mid \widehat{x} \in \mathbb{Z}_4\} = \{\widehat{0} + N, \widehat{1} + N, \widehat{2} + N, \widehat{3} + N\} = \{N, \widehat{1} + N\} = \{\{\widehat{0}, \widehat{2}\}, \{\widehat{1}, \widehat{3}\}\}.$$

Let us fill in the operation table for the factor group $\mathbb{Z}_4/N$:

$+$	$N = \{\widehat{0}, \widehat{2}\}$	$\widehat{1} + N = \{\widehat{1}, \widehat{3}\}$
$N = \{\widehat{0}, \widehat{2}\}$	$\{\widehat{0}, \widehat{2}\}$	$\{\widehat{1}, \widehat{3}\}$
$\widehat{1} + N = \{\widehat{1}, \widehat{3}\}$	$\{\widehat{1}, \widehat{3}\}$	$\{\widehat{0}, \widehat{2}\}$