for an $a \in \{1, \ldots, l\}$. Hence the jth line is mapped onto the set

$$\{gg_j m_1 \mathcal{U}, \ldots, gg_j m_k \mathcal{U}\} = \{g_a m_1 \mathcal{U}, \ldots, g_a m_k \mathcal{U}\}.$$

Definition 1.5.5.1.1. Let $\mathcal{G}$ be a group and X a $\mathcal{G}$-set.

(i) A *congruence* $\{S_1, \ldots, S_l\}$ on X is a partition of X into non-empty subsets $X = \dot{\bigcup}_{i=1}^{l} S_i$ such that for all $x_1, x_2 \in S_i$, $g \in \mathcal{G}$, $gx_1 \in S_j$ implies $gx_2 \in S_j$.

(ii) The congruences $\{X\}$ and $\{\{x\} \mid x \in X\}$ are called the *trivial congruences*.

(iii) X is called a *primitive* $\mathcal{G}$-set if $\mathcal{G}$ is transitive on X, $|X| > 1$ and X has only the trivial congruences. □

Hence the considerations above have proven the following lemma.

Lemma 1.5.5.1.2. Let $\mathcal{M} \le \mathcal{G}$ be a subgroup of the group $\mathcal{G}$. Then $\mathcal{M}$ is a maximal subgroup if and only if the $\mathcal{G}$-set $\mathcal{G}/\mathcal{M}$ is primitive. □

The advantage of this point of view is that the groups $\mathcal{G}$ having a faithful, primitive, finite $\mathcal{G}$-set have a special structure. It will turn out that this structure is very similar to the structure of space groups.

If X is a $\mathcal{G}$-set and $\mathcal{N} \trianglelefteq \mathcal{G}$ is a normal subgroup of $\mathcal{G}$, then $\mathcal{G}$ acts on the set of $\mathcal{N}$-orbits on X, hence $\{\mathcal{N}x \mid x \in X\}$ is a congruence on X. If X is a primitive $\mathcal{G}$-set, then this congruence is trivial, hence $\mathcal{N}x = \{x\}$ or $\mathcal{N}x = X$ for all $x \in X$. This means that $\mathcal{N}$ either acts trivially or transitively on X.

One obtains the following:

Theorem 1.5.5.1.3. [Theorem of Galois (*ca* 1830).]
Let $\mathcal{H}$ be a finite group and let X be a faithful, primitive $\mathcal{H}$-set. Assume that $\{e\} \neq \mathcal{N} \trianglelefteq \mathcal{H}$ is an Abelian normal subgroup. Then

(*a*) $\mathcal{N}$ is a minimal normal subgroup of $\mathcal{H}$ (*i.e.* for all $\mathcal{N}_1 \trianglelefteq \mathcal{H}$, $\mathcal{N}_1 \subseteq \mathcal{N} \Leftrightarrow \mathcal{N}_1 = \mathcal{N}$ or $\mathcal{N}_1 = \{e\}$).

(*b*) $\mathcal{N}$ is an elementary Abelian p-group for some prime p and $|X| = |\mathcal{N}|$ is a prime power.

(*c*) $\mathcal{C}_{\mathcal{H}}(\mathcal{N}) = \mathcal{N}$ and $\mathcal{N}$ is the unique minimal normal subgroup of $\mathcal{H}$. □

Proof. Let $\{e\} \neq \mathcal{N} \trianglelefteq \mathcal{H}$ be an Abelian normal subgroup. Then $\mathcal{N}$ acts faithfully and transitively on X. To establish a bijection between the sets $\mathcal{N}$ and X, choose $x \in X$ and define $\varphi : \mathcal{N} \to X; n \mapsto n \cdot x$. Since $\mathcal{N}$ is transitive, φ is surjective. To show the injectivity of φ, let $n_1, n_2 \in \mathcal{N}$ with $\varphi(n_1) = \varphi(n_2)$. Then $n_1 \cdot x = n_2 \cdot x$, hence $n_1^{-1} n_2 x = x$. But then $n_1^{-1} n_2$ acts trivially on X, because if $y \in X$ then the transitivity of $\mathcal{N}$ implies that there is an $n \in \mathcal{N}$ with $n \cdot x = y$. Then $n_1^{-1} n_2 \cdot y = n_1^{-1} n_2 n \cdot x = n n_1^{-1} n_2 \cdot x = n \cdot x = y$, since $\mathcal{N}$ is Abelian. Since X is a faithful $\mathcal{H}$-set, this implies $n_1^{-1} n_2 = e$ and therefore $n_1 = n_2$. This proves $|\mathcal{N}| = |X|$. Since this equality holds for all nontrivial Abelian normal subgroups of $\mathcal{H}$, statement (*a*) follows. If p is some prime dividing $|\mathcal{N}|$, then the Sylow p-subgroup of $\mathcal{N}$ is normal in $\mathcal{N}$, since $\mathcal{N}$ is Abelian. Therefore it is also a characteristic subgroup of $\mathcal{N}$ and hence a normal subgroup in $\mathcal{H}$ (see the remarks below Definition 1.5.3.5.3). Since $\mathcal{N}$ is a minimal normal subgroup of $\mathcal{H}$, this implies that $\mathcal{N}$ is equal to its Sylow p-subgroup. Therefore, the order of $\mathcal{N}$ is a prime power $|\mathcal{N}| = p^r$ for some prime p and $r \in \mathbb{N}$. Similarly, the set $\mathcal{N}^p := \{n^p \mid n \in \mathcal{N}\}$ is a normal subgroup of $\mathcal{H}$ properly contained in $\mathcal{N}$. Therefore $\mathcal{N}^p = \{e\}$ and $\mathcal{N}$ is elementary Abelian. This establishes (*b*).
To see that (*c*) holds, let $g \in \mathcal{C}_{\mathcal{H}}(\mathcal{N})$. Choose $x \in X$. Then $g \cdot x = y \in X$. Since $\mathcal{N}$ acts transitively, there is an $n \in \mathcal{N}$ such that $n \cdot x = y$. Hence $n^{-1} g \cdot x = x$. As above, let $z \in X$ be any element of X. Then there is an element $n_1 \in \mathcal{N}$ with $z = n_1 \cdot x$. Hence $n^{-1} g \cdot z = n^{-1} g n_1 \cdot x = n_1 n^{-1} g \cdot x = n_1 \cdot x = z$. Since z was arbitrary and X is faithful, this implies that $g = n \in \mathcal{N}$. Therefore $\mathcal{C}_{\mathcal{H}}(\mathcal{N}) \subseteq \mathcal{N}$. Since $\mathcal{N}$ is Abelian, one has $\mathcal{N} \subseteq \mathcal{C}_{\mathcal{H}}(\mathcal{N})$, hence $\mathcal{N} = \mathcal{C}_{\mathcal{H}}(\mathcal{N})$. To see that $\mathcal{N}$ is unique, let $\mathcal{P} \neq \mathcal{N}$ be another normal subgroup of $\mathcal{H}$. Since $\mathcal{N}$ is a minimal normal subgroup, one has $\mathcal{N} \cap \mathcal{P} = \{e\}$, and therefore for $p \in \mathcal{P}$, $n \in \mathcal{N}$: $n^{-1} p^{-1} n p \in \mathcal{N} \cap \mathcal{P} = \{e\}$. Hence $\mathcal{P}$ centralizes $\mathcal{N}$, $\mathcal{P} \subseteq \mathcal{C}_{\mathcal{H}}(\mathcal{N}) = \mathcal{N}$, which is a contradiction. QED

Hence the groups $\mathcal{H}$ that satisfy the hypotheses of the theorem of Galois are certain subgroups of an affine group $\mathcal{A}_n(\mathbb{Z}/p\mathbb{Z})$ over a finite field $\mathbb{Z}/p\mathbb{Z}$. This affine group is defined in a way similar to the affine group $\mathcal{A}_n$ over the real numbers where one has to replace the real numbers by this finite field. Then $\mathcal{N}$ is the translation subgroup of $\mathcal{A}_n(\mathbb{Z}/p\mathbb{Z})$ isomorphic to the n-dimensional vector space

$$(\mathbb{Z}/p\mathbb{Z})^n = \{\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \ldots, x_n \in \mathbb{Z}/p\mathbb{Z}\}$$

over $\mathbb{Z}/p\mathbb{Z}$. The set X is the corresponding affine space $\mathbb{A}_n(\mathbb{Z}/p\mathbb{Z})$. The factor group $\overline{\mathcal{H}} = \mathcal{H}/\mathcal{N}$ is isomorphic to a subgroup of the linear group of $(\mathbb{Z}/p\mathbb{Z})^n$ that does not leave invariant any non-trivial subspace of $(\mathbb{Z}/p\mathbb{Z})^n$.

1.5.5.2. *Soluble groups*

Definition 1.5.5.2.1. Let $\mathcal{G}$ be a group. The *derived series* of $\mathcal{G}$ is the series $(\mathcal{G}_0, \mathcal{G}_1, \ldots)$ defined *via* $\mathcal{G}_0 := \mathcal{G}$, $\mathcal{G}_i := \langle g^{-1} h^{-1} g h \mid g, h \in \mathcal{G}_{i-1} \rangle$. The group $\mathcal{G}_1$ is called the *derived subgroup* of $\mathcal{G}$. The group $\mathcal{G}$ is called *soluble* if $\mathcal{G}_n = \{e\}$ for some $n \in \mathbb{N}$. □

Remarks

(i) The $\mathcal{G}_i$ are characteristic subgroups of $\mathcal{G}$.

(ii) $\mathcal{G}$ is Abelian if and only if $\mathcal{G}_1 = \{e\}$.

(iii) $\mathcal{G}_1$ is characterized as the smallest normal subgroup of $\mathcal{G}$, such that $\mathcal{G}/\mathcal{G}_1$ is Abelian, in the sense that every normal subgroup of $\mathcal{G}$ with an Abelian factor group contains $\mathcal{G}_1$.

(iv) Subgroups and factor groups of soluble groups are soluble.

(v) If $\mathcal{N} \trianglelefteq \mathcal{G}$ is a normal subgroup, then $\mathcal{G}$ is soluble if and only if $\mathcal{G}/\mathcal{N}$ and $\mathcal{N}$ are both soluble.

Example 1.5.5.2.2.
The derived series of $\mathcal{C}yc_2 \times \mathcal{S}ym_4$ is:

$$\mathcal{C}yc_2 \times \mathcal{S}ym_4 \trianglerighteq \mathcal{A}lt_4 \trianglerighteq \mathcal{C}yc_2 \times \mathcal{C}yc_2 \trianglerighteq \mathcal{I}$$

(or in Hermann–Mauguin notation $m\overline{3}m \trianglerighteq 23 \trianglerighteq 222 \trianglerighteq 1$) and that of $\mathcal{C}yc_2 \times \mathcal{C}yc_2 \times \mathcal{S}ym_3$ is

$$\mathcal{C}yc_2 \times \mathcal{C}yc_2 \times \mathcal{S}ym_3 \trianglerighteq \mathcal{C}yc_3 \trianglerighteq \mathcal{I}$$

(Hermann–Mauguin notation: $6/mmm \trianglerighteq 3 \trianglerighteq 1$).
Hence these two groups are soluble. (For an explanation of the groups that occur here and later, see Section 1.5.3.6.)

Now let $\mathcal{R} \le \mathcal{E}_3$ be a three-dimensional space group. Then $\mathcal{T}(\mathcal{R})$ is an Abelian normal subgroup, hence $\mathcal{T}(\mathcal{R})$ is soluble. The factor group $\mathcal{R}/\mathcal{T}(\mathcal{R})$ is isomorphic to a subgroup of either $\mathcal{C}yc_2 \times \mathcal{S}ym_4$ or $\mathcal{C}yc_2 \times \mathcal{C}yc_2 \times \mathcal{S}ym_3$ and therefore also soluble. Using the remark above, one deduces that all three-dimensional space groups are soluble.

Lemma 1.5.5.2.3. Let $\mathcal{R}$ be a three-dimensional space group. Then $\mathcal{R}$ is soluble. □

references