Preliminaries involving permutation groups. Let G be a permutation group upon a set Ω. Fix an element $\omega \in \Omega$. The set of all $g \in G$ that fixes ω is said to be the *stabilizer* of G at ω. It is a subgroup and is denoted by G_ω.

Lemma 1. *Suppose that $g \in G$ and $\alpha = g(\omega)$. Then $G_\alpha = gG_\omega g^{-1}$. If G is transitive, then $G_\omega \cap Z(G) = 1$.*

Proof. Let h be an element of G. Then $h \in G_\alpha \Leftrightarrow h(\alpha) = \alpha \Leftrightarrow hg(\omega) = g(\omega) \Leftrightarrow g^{-1}hg(\omega) = \omega \Leftrightarrow g^{-1}hg \in G_\omega \Leftrightarrow h \in gG_\omega g^{-1}$. Suppose that G is transitive and that $h \in Z(G)$ fixes ω. Since G is transitive, for each $\alpha \in \Omega$ there exists $g \in G$ such that $g(\omega) = \alpha$. Since $h \in G_\omega$, $ghg^{-1} \in G_\alpha$. Therefore $h = ghg^{-1} \in G_\alpha$. Hence $h(\alpha) = \alpha$ for each $\alpha \in \Omega$. Thus $h = \mathrm{id}_\Omega$. □

Recall that if S is a subset of a group G, then $N_G(S) = \{g \in G;\ gSg^{-1} = S\}$ is called the *normalizer* of S, and $C_G(S) = \{g \in G;\ gs = sg \text{ for all } s \in S\}$ the *centralizer* of S. Both $N_G(S)$ and $C_G(S)$ are subgroups of G. To prove that $H \leq G$ is a subgroup of $N_G(S)$ it suffices to verify that $hSh^{-1} \subseteq S$ for every $h \in H$. Indeed, $h^{-1}S(h^{-1})^{-1} \subseteq S$ is the same as $S \subseteq hSh^{-1}$. Similarly for centralizers.

Lemma 2. *Let g be an element of G. Then $G_{g(\omega)} = G_\omega$ if and only if $g \in N_G(G_\omega)$.*

Proof. By Lemma 1, $G_{g(\omega)} = G_\omega$ if and only if $gG_\omega g^{-1} = G_\omega$, which is the same as $g \in N_G(G_\omega)$. □

Lemma 3. *Let h and g be elements of G. Then $hG_\omega = gG_\omega$ if and only if $g(\omega) = h(\omega)$, while $G_\omega h = G_\omega g$ if and only if $g^{-1}(\omega) = h^{-1}(\omega)$.*

Proof. Since $(G_\omega h)^{-1} = h^{-1}G_\omega$, only the first equality needs to be verified. Now, $hG_\omega = gG_\omega \Leftrightarrow h^{-1}g \in G_\omega \Leftrightarrow h^{-1}g(\omega) = \omega \Leftrightarrow g(\omega) = h(\omega)$. □

A set $\Gamma \subseteq \Omega$ is said to be a *block* (of G) if it is nonempty and satisfies the implication

$$g(\gamma) \in \Gamma \Rightarrow g(\Gamma) \subseteq \Gamma$$

for all $g \in G$ and $\gamma \in \Gamma$.

Lemma 4. *Let Γ be a block. If $g \in G$, then either $g(\Gamma) = \Gamma$ or $g(\Gamma) \cap \Gamma = \emptyset$. In any case, $g(\Gamma)$ is a block of G as well.*

Proof. Suppose first that there exist $\beta, \gamma \in \Gamma$ such that $g(\gamma) = \beta$. Then $g(\Gamma) \subseteq \Gamma$ by the definition of a block. Since $g^{-1}(\beta) = \gamma$, $\gamma^{-1}(\Gamma) \subseteq \Gamma$ too. Hence $g(\Gamma) = \Gamma$. We have proved that this is true whenever $\gamma(\Gamma) \cap \Gamma \neq \emptyset$.

To prove that $g(\Gamma)$ is always a block, consider $\alpha \in g(\Gamma)$ and $h \in G$ such that $h(\alpha) = \beta \in g(\Gamma)$. Then $hg(g^{-1}(\alpha)) = g(g^{-1}(\beta))$, and thus $g^{-1}hg(g^{-1}(\alpha)) = g^{-1}(\beta)$. Both $g^{-1}(\alpha)$ and $g^{-1}(\beta)$ belong to Γ. Therefore $g^{-1}hg(\Gamma) = \Gamma$, which means $h(g(\Gamma)) = g(\Gamma)$. We have shown that $g(\Gamma)$ is a block. □

Blocks Γ_1 and Γ_2 are said to be *conjugate* if there exists $g \in G$ such that $g(\Gamma_1) = \Gamma_2$. The relation 'to be conjugate' clearly is an equivalence upon the set of all blocks of G.

Corollary 5. *Suppose that G is transitive. If Γ is a block of G, then the set of all $g(\Gamma)$, $g \in G$, partitions the set Ω. Furthermore, two blocks are conjugate if and only if they induce the same partition of Ω.*

Proof. Indeed, the transitivity ensures that the sets $g(\Gamma)$ are blocks that cover all of Ω. Moreover, any two such blocks are conjugate. The rest follows from Lemma 4 in an immediate fashion. □

An equivalence $\sim$ of Ω is said to be *stable under* G if

$$\alpha \sim \beta \ \Leftrightarrow\ g(\alpha) \sim g(\beta) \text{ for each } \alpha, \beta \in \Omega \text{ and } g \in G.$$

In fact it is enough to prove that the implication

$$\alpha \sim \beta \ \Rightarrow\ g(\alpha) \sim g(\beta) \text{ for each } \alpha, \beta \in \Omega \text{ and } g \in G.$$

is satisfied, since then $g(\alpha) \sim g(\beta)$ implies $\alpha = g^{-1}g(\alpha) \sim g^{-1}g(\beta) = \beta$.

Lemma 6. *Let $\sim$ be a stable equivalence. If $\alpha \in \Omega$ and $g \in G$, then $[\alpha]_\sim$ and $[g(\alpha)]_\sim$ are conjugate blocks. If G is transitive, then the blocks of $\sim$ form a partition of Ω by conjugate blocks. On the other hand, every such partition induces a stable equivalence.*

Proof. By the definition of stable equivalence, $g([\alpha]_\sim) = [g(\alpha)]_\sim$, for every $\alpha \in \Omega$ and each $g \in G$. If $\Gamma = [\omega]_\sim$ and $g(\omega) \in \Gamma$, then $g(\Gamma) = \Gamma$. Hence each block of $\sim$ is a block of G. The rest follows from Corollary 5. □

Lemma 7. *For $\alpha, \beta \in \Omega$ set $\alpha \sim \beta \Leftrightarrow G_\alpha = G_\beta$. The equivalence $\sim$ is stable under G. Furthermore, suppose that G is transitive, that $\omega \in G$ and that $\Gamma = \{\alpha \in \Omega;\ G_\omega \subseteq G_\alpha\}$. If Γ is a block of G, then $\Gamma = [\omega]_\sim$.*

Proof. If $G_\alpha = G_\beta$ and $g \in G$, then $G_{g(\alpha)} = G_{g(\beta)}$, by Lemma 1. Suppose now that G is transitive and that ω and Γ are as in the statement. Suppose that $\alpha \in \Gamma$ and let $g \in G$ be such that $g(\omega) = \alpha$. Then $G_\omega \subseteq gG_\omega g^{-1} = G_\alpha$, by Lemma 1 and the definition of Γ. Since $g(\Gamma) = \Gamma$ there is also $g^{-1}(\omega) \in \Gamma$, and so $G_\omega \subseteq g^{-1}G_\omega g$. Therefore $G_\omega = gG_\omega g^{-1} = G_\alpha$. □

The following characterization of blocks is nearly self-evident. Note that it differs from the definition of a block by considering the defining property just for one element, i.e. the element ω.

Lemma 8. *Suppose that Γ is a subset of the orbit $G(\omega)$ that contains ω. The following is equivalent:*

(1) *Γ is a block;*
(2) *the ensuing implication holds for all $g \in G$:*

$$g(\omega) \in \Gamma \ \Rightarrow\ g(\Gamma) \subseteq \Gamma \text{ and } g^{-1}(\omega) \in \Gamma;$$

(3) *the ensuing implication holds for all $g \in G$:*

$$g(\omega) \in \Gamma \ \Rightarrow\ g(\Gamma) = \Gamma.$$

Proof. Points (2) and (3) are equivalent since if (2) holds, then $g^{-1}(\omega) \in \Gamma$ implies $g^{-1}(\Gamma) \subseteq \Gamma$. If Γ is a block, then (3) holds, by Lemma 4. For the converse assume that $g(\gamma) \in \Gamma$ for some $\gamma \in \Gamma$ and $g \in G$. Since $\Gamma \subseteq G(\omega)$, there exists $h \in G$ such that $h(\omega) = \gamma$. This gives $h(\Gamma) = \Gamma$, $gh(\omega) \in \Gamma$ and $gh(\Gamma) = \Gamma$. Hence $g(\Gamma) = \Gamma$. □

Lemma 9. *Let $H \leq G$ be such that $G_\omega \leq H$. Then $\Gamma = H(\omega)$ (the orbit of ω under the action of H) is a block of G, and $H = \{g \in G;\ g(\omega) \in \Gamma\}$.*

Proof. Let $g \in G$ be such that $g(\omega) \in H(\omega)$. Then $g(\omega) = h(\omega)$ for some $h \in H$. Therefore $h^{-1}g \in G_\omega \leq H$, and thus $g \in H$. Hence $g(H(\omega)) = (gH)(\omega) = H(\omega)$. That makes $H(\omega)$ a block. If $g(\omega) \in \Gamma$, $g \in G$, then there exists $h \in H$ such that $g(\omega) = h(\omega)$. Hence $h^{-1}g \in G_\omega \leq H$, and so $g = h(h^{-1}g) \in H$. □

Lemma 10. *Let $\Gamma \subseteq G(\omega)$ be a block of G such that $\omega \in \Gamma$. Put $H = \{h \in G;\ h(\omega) \in \Gamma\}$. Then H is a subgroup of G that contains G_ω, and $\Gamma = H(\omega)$.*

Proof. Since Γ is a block within the orbit of ω, there has to be $H = \{h \in G; h(\Gamma) = \Gamma\}$, by Lemma 8. This implies that H is a subgroup of G and that $\Gamma = H(\omega)$. □

Note that $\{\omega\}$ is always a block of G and that the orbit $G(\omega)$ is also a block.

Lemmas 9 and 10 establish a 1-to-1 correspondence between blocks $\Gamma \subseteq G(\omega)$ that include ω, and subgroups of G that contain G_ω. The correspondence respects inclusions. Hence it yields an isomorphism between the lattice of blocks that are subsets of $G(\omega)$ and contain ω, and the interval $[G_\omega, G]$ in the lattice of all subgroups of G. If $G(\omega) \neq \{\omega\}$, then $G_\omega \neq G$. In such a case the interval $[G_\omega, G]$ contains only two elements (two subgroups) if and only if there exists no block that is a proper subset of $G(\omega)$ and contains at least two elements.

The permutation group G is said to be *primitive* if it is nontrivial and the only blocks of G are Ω and $\{\alpha\}$, $\alpha \in \Omega$. Since $G(\omega)$ is a block, a primitive group has to be transitive. In view of the correspondence described above, the following claim may be stated without a proof.

Lemma 11. *A nontrivial transitive permutation group G is primitive if and only if G_ω is a maximal subgroup of G.*

Lemma 12. *If $H \trianglelefteq G$ and Γ is an orbit of H, then Γ is a block.*

Proof. Suppose that $\omega \in \Gamma$ and put $K = HG_\omega$. If $k \in K$, then there exists $h \in H$ such that $k(\omega) = h(\omega)$. Thus $\Gamma = K(\omega)$. The statement follows from Lemma 9. □

Lemma 13. *Let $\sim$ be the equivalence upon Ω given by $G_\alpha = G_\beta$. Assume that G is transitive and put $\Gamma = [\omega]_\sim$. Then Γ is a block of G, and $\{g \in G;\ g(\omega) \in \Gamma\} = N_G(G_\omega)$.*

Proof. The set Γ is a block by Lemmas 7 and 6. By Lemma 2, $\Gamma = N_G(G_\omega)(\omega)$. The rest follows from Lemma 9 since $N_G(G_\omega)$ contains G_ω. □

Suppose that $U \leq V$ are groups and that $S \subseteq V$. Call S a *left transversal* to U in V if $SU = V$, $1 \in S$, and $s_1U = s_2U \Rightarrow s_1 = s_2$, whenever $s_1, s_2 \in S$. The *right transversal* is defined in a mirror way. A set that is both left and right transversal is known as a *two-sided tranversal*, or just a *transversal*. The notion of transversal is sometimes defined without stipulating that the transversal contains the unit element 1.

The *core* of U in V is the greatest normal subgroup $N \trianglelefteq V$ that is contained in U. Note that $N = \bigcap_{g \in V} gUg^{-1}$.

Lemma 14. *Let S be a subset of G that contains* id_G. *S is the left transversal to G_ω in G if and only if for each $\alpha \in G(\omega)$ there exists exactly one $s \in S$ such that $s(\omega) = \alpha$. Similarly, the set S is the right transversal to G_ω in G if and only if for each $\alpha \in G(\omega)$ there exists exactly one $s \in S$ such that $s(\alpha) = \omega$.*

Proof. This follows from the description of cosets of G_ω, as given in Lemma 3. □

Lemma 15. *If G is transitive, then the core of G_ω is trivial.*

Proof. By Lemma 1, the core of G_ω is equal to the intersection of all G_α, $\alpha \in \Omega$. Of course, the only permutation that fixes each $\alpha \in \Omega$ is the identity. □

Proposition 16. *Suppose that T is a left transversal to G_ω in G, and that $X \subseteq G$ generates G. For each $\alpha \in G(\omega)$ denote by t_α that element of T which sends ω upon α. Then*

$$G_\omega = \langle t_{x(\alpha)}^{-1} x t_\alpha;\ \alpha \in G(\omega) \text{ and } x \in X\rangle.$$

Proof. For $S \subseteq G$ set $S^{\pm 1} = \{s, s^{-1};\ s \in S\}$. Each element of G may be thus expressed as $x_n \cdots x_1$, where $x_i \in X^{\pm 1}$, $1 \leq i \leq n$. Denote by Y the set of all elements $t_{x(\alpha)}^{-1}xt_\alpha$, $\alpha \in G(\omega)$ and $x \in X$. If $\beta = x(\alpha)$, then the inverse of such an element is equal to $t_{x^{-1}(\beta)}^{-1}x^{-1}t_\beta$. Hence

$$Y^{\pm 1} = \{t_{x(\alpha)}^{-1}xt_\alpha;\ \alpha \in G(\omega) \text{ and } x \in X^{\pm 1}\}.$$

Note that $Y^{\pm 1} \subseteq G_\omega$ and that $t_\omega = \mathrm{id}_\Omega$.

Suppose now that $g = x_n \cdots x_1 \in G_\omega$, where $x_1, \dots, x_n \in X^{\pm 1}$. Put $\alpha_i = x_i \cdots x_1(\omega)$, $0 \le i < n$, and insert $t_{\alpha_i}t_{\alpha_i}^{-1} = t_{\alpha_i}t_{x_i(\alpha_{i-1})}^{-1}$ in between x_{i+1} and x_i, $1 \le i < n$. That makes

$$g = t_\omega g t_\omega = t_\omega^{-1} x_n \cdots x_1 t_\omega = \left(t_{x_n(\alpha_{n-1})}^{-1} x_n t_{\alpha_{n-1}}\right) \cdots \left(t_{x_1(\alpha_0)}^{-1} x_1 t_{\alpha_0}\right)$$

an element of $\langle Y \rangle$. □

Quasigroup congruences. Let Q be a quasigroup. Set

$$\mathrm{LMlt}(Q) = \langle L_x;\ x \in Q \rangle,$$
$$\mathrm{RMlt}(Q) = \langle R_x;\ x \in Q \rangle \text{ and}$$
$$\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q \rangle.$$

Call these groups the *left multiplication group*, the *right multiplication group* and the *multiplication group* of Q, respectively.

Proposition 17. *Let Q be a quasigroup. An equivalence $\sim$ on Q is a congruence if and only if for all $x, y, z \in Q$*

$$x \sim y \ \Rightarrow\ xz \sim yz,\ zx \sim zy,\ x/z \sim y/z \text{ and } z\backslash x = z\backslash y.$$

Proof. If $*$ is a binary operation on Q, then $\sim$ is compatible with $*$ if and only if $x \sim y \Rightarrow x * z \sim y * z$ and $z * x \sim z * y$ holds for all $x, y, z \in Q$. To see that this is true consider $a, b, c, d \in Q$ such that $a \sim b$ and $c \sim d$. If the implication holds for all $x, y, z \in Q$, then $a * c \sim b * c \sim b * d$.

Due to this fact the proof may be restricted to verifying implications $x \sim y \Rightarrow z/x \sim z/y$ and $x \sim y \Rightarrow x\backslash z \sim y\backslash z$. It is enough to prove the latter implication because of mirror symmetry. Before doing so let us observe that all implications assumed may be considered as equivalences. E.g., we have $x \sim y \Leftrightarrow xz \sim yz$. To prove the converse direction suppose that $xz \sim yz$. By the assumptions of the statement $(xz)/z \sim (yz)/z$. However $(xz)/z = x$ and $(yz)/z = y$. Similarly in the other cases.

Thus $x\backslash z \sim y\backslash z \Leftrightarrow z \sim x(y\backslash z) \Leftrightarrow z/(y\backslash z) \sim (x(y\backslash z))/(y\backslash z)$. Now, $z/(y\backslash z) = y$ and $x(y\backslash z))/(y\backslash z) = x$. □

Theorem 18. *Let Q be a quasigroup and let $\sim$ be an equivalence upon Q. The equivalence $\sim$ is a congruence of Q if and only if it is stable under* $\mathrm{Mlt}(Q)$.

Proof. The equivalence $\sim$ is stable under $\mathrm{Mlt}(Q)$ if $x \sim y$ implies $g(x) \sim g(y)$ for each $x, y \in Q$ and $g \in G$. For the implication to hold it suffices if it holds for generators of $\mathrm{Mlt}(Q)$ and the inverses of these generators. That follows from Proposition 17 since $R_z(x) = xz$, $L_z(x) = zx$, $R_z^{-1}(x) = x/z$ and $L_z^{-1}(x) = z\backslash x$. □

Corollary 19. *Let S be a nonempty subset of a quasigroup Q. The set S is a block of a congruence if and only if it is a block of* $\mathrm{Mlt}(Q)$. *Each such block determines exactly one congruence of Q.*

Proof. Indeed, blocks of a stable equivalence are blocks of the permutation group, and each block of a transitive group fully determines a stable equivalence. □

Corollary 20. *Let Q be a quasigroup, $|Q| > 1$. The quasigroup is simple if and only if* $\mathrm{Mlt}(Q)$ *is a primitive permutation group.*

Proof. Recall that a transitive group is said to be primitive if it possesses no non-trivial block (i.e., a block that differs from the underlying set and contains more than than one element.) □

Inner mapping group. Let Q be a loop. The stabilizer $(\mathrm{Mlt}\, Q)_1$ is known as the *inner mapping group*. It is denoted by $\mathrm{Inn}(Q)$. Thus $\varphi \in \mathrm{Inn}(Q)$ if and only if $\varphi(1) = 1$ and $\varphi \in \mathrm{Mlt}(Q)$.

Theorem 21. *Let Q be a loop. Then* $\mathrm{Inn}(Q) = \langle L_{xy}^{-1} L_x L_y, R_{yx}^{-1} R_x R_y, R_x^{-1} L_x;\ x, y \in Q\rangle$.

Proof. Use Proposition 16 with $G = \mathrm{Mlt}(Q)$, $X = \{L_y, R_y;\ y \in Q\}$ and $T = \{L_y;\ y \in Q\}$. Note that T is indeed a (left) transversal to $\mathrm{Inn}(Q)$ since $L_y(1) = y$ for every $y \in Q$, and $L_1 = \mathrm{id}_Q$.

By Proposition 16 the set of all $L_{xy}^{-1} L_x L_y$ and $L_{yx}^{-1} R_x L_y$ generate $\mathrm{Inn}(Q)$. Obviously, $R_x^{-1} L_x \in \mathrm{Inn}(Q)$. The rest follows from $L_y = R_y(R_y^{-1} L_y)$ and $L_{yx}^{-1} = (R_{yx}^{-1} L_{yx})^{-1} R_{yx}^{-1}$. □

Mappings $L_{xy}^{-1} L_x L_y$, $R_{yx}^{-1} R_x R_y$, $R_x^{-1} L_x$ are known as the *standard generators* of $\mathrm{Inn}(Q)$. There are many other mappings that belong to $\mathrm{Inn}(Q)$. For example $[L_x, R_y] = L_x^{-1} R_y^{-1} L_x R_y \in \mathrm{Inn}(Q)$ for all $x, y \in Q$.

Normal subloops. Let $\sim$ be a congruence of a loop Q. If $x \sim 1$ and $y \sim 1$, then $xy \sim 1$, $x/y \sim 1$ and $x\backslash y \sim 1$ since $1 = 1 \cdot 1 = 1/1 = 1\backslash 1$. The set $[\sim]_1$ is thus a subloop of Q.

A subloop of a loop Q is called *normal* if it is a block of a congruence. By Corollary 19 the normal subloop determines exactly one congruence of Q. Denote the congruence by $\sim$. Blocks of $\sim$ are the blocks of $\mathrm{Mlt}(Q)$ conjugate to $N = [1]_\sim$. Hence they are equal to $L_x(N) = xN = Nx = R_x(N)$. A block $xN = Nx$ is called a *coset* of N. The fact that N is a normal subloop of Q is denoted, like in groups, by $N \trianglelefteq Q$.

Theorem 22. *Let Q be a loop and let N be a subloop of Q. The following is equivalent:*

(i) *N is normal;*
(ii) *$\varphi(N) \subseteq N$ for each $\varphi \in \mathrm{Inn}(Q)$;*
(iii) *$\varphi(N) = N$ for each $\varphi \in \mathrm{Inn}(Q)$;*
(iv) *$xN = Nx$, $x(yN) = (xy)N$ and $(Ny)x = N(yx)$ for all $x, y \in Q$.*

Proof. If N is a block of a congruence $\sim$, $x \in N$ and $\varphi \in \mathrm{Inn}(Q)$, then $1 = \varphi(1) \sim \varphi(x)$. Hence (i) ⇒ (ii). If (ii) holds and $\varphi \in \mathrm{Inn}(Q)$, then both $\varphi(N) \subseteq N$ and $\varphi^{-1}(N) \subseteq N$ are true. Thus $\varphi(N) = N$, and (ii) ⇒ (iii). The condition (iv) can be also expressed as $L_{xy}^{-1} L_x L_y(N) = N$, $R_{yx}^{-1} R_x R_y(N) = N$ and $R_x^{-1} L_x(N) = N$. In view of Theorem 21 this means that (iii) ⇔ (iv).

It remains to prove (iii) ⇒ (i). Each element of $\mathrm{Mlt}(Q)$ may be written as $L_x\varphi$, where $\varphi \in \mathrm{Inn}(Q)$ and $x \in Q$. (This is because the set of all left translations forms a transversal to $\mathrm{Inn}(Q)$.) If $x \in N$, then $L_x\varphi(N) = xN = N$. If $x \notin N$, then $L_x\varphi(N) = xN$ and $xN \cap N = \emptyset$. This means that N is a block of $\mathrm{Mlt}(Q)$. □

Centres. Recall that the *centre* of a loop Q is defined as the set of all $z \in Q$ such that $z \in N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$ and that $zx = xz$ for all $x \in Q$.

The following facts are direct enough to be stated without a proof.

Lemma 23. *Let a be an element of a loop Q. Then*

(1) *$a \in N_\lambda \Leftrightarrow R_{yx}^{-1} R_x R_y(a) = a$ for all $x, y \in Q$;*
(2) *$a \in N_\mu \Leftrightarrow [L_x, R_y](a) = a$ for all $x, y \in Q$; and*

(3) $a \in N_\rho \Leftrightarrow L_{xy}^{-1}L_xL_y(a) = a$ *for all* $x, y \in Q$;

Theorem 24. *Let Q be a loop. Then $Z(Q)$ is a normal subloop of Q. An element $z \in Q$ belongs to $Z(Q)$ if and only if $\varphi(z) = z$ for all $\varphi \in \mathrm{Inn}(Q)$. Furthermore, $Z(\mathrm{Mlt}(Q)) = \{L_z;\ z \in Z(Q)\} = \{R_z;\ z \in Z(Q)\}$ and $N_{\mathrm{Mlt}(Q)}(\mathrm{Inn}(Q)) = \mathrm{Inn}(Q)Z(\mathrm{Mlt}(Q))$.*

Proof. If $a \in Z(Q)$, then a is fixed by every standard generator of $\mathrm{Inn}(Q)$, by Lemma 23 and Theorem 21. Thus each $\varphi \in \mathrm{Inn}(Q)$ fixes every $a \in Z(Q)$. For the converse direction use Lemma 23 and observe again that $T_x(a) = a \Leftrightarrow ax = xa$.

Since $N(Q)$ is a subloop of Q, the product ab belongs to $N(Q)$ for all $a, b \in Z(Q)$. Therefore $L_{ab} = L_aL_b = R_aR_b = R_{ba} = R_{ab}$. Also, $L_{a^{-1}} = L_a^{-1} = R_a^{-1} = R_{a^{-1}}$. Hence $Z(Q)$ is a subloop of Q. Since $\mathrm{Inn}(Q)$ fixes each element of $a \in Z(Q)$ it has to be a normal subloop, by Theorem 22. That makes $Z(Q)$ a block of $\mathrm{Mlt}(Q)$. Elements $z \in Z(Q)$ have been characterized as those elements of Q that are fixed by each $\varphi \in \mathrm{Inn}(Q)$. In other words $z \in Z(Q) \Leftrightarrow \mathrm{Inn}(Q) \subseteq (\mathrm{Mlt}(Q))_z$. By Lemma 7, $z \in Z(Q) \Leftrightarrow \mathrm{Inn}(Q) = (\mathrm{Mlt}(Q))_z$.

If $z \in Z(Q)$, then $L_z = R_z$ and both $L_zR_x = R_xL_z$ and $R_zL_x = L_xR_z$ are clearly true for each $x \in Q$. Hence $L_z \in Z(\mathrm{Mlt}(Q))$. If $\psi \in Z(\mathrm{Mlt}(Q))$ and $\varphi \in \mathrm{Inn}(Q)$, then $\varphi(\psi(1)) = \psi(\varphi(1)) = \psi(1)$. Hence $\psi(1) = z \in Z(Q)$, and $L_z^{-1}\psi \in \mathrm{Inn}(Q)$. No nontrivial element of $\mathrm{Inn}(Q)$ may be central, say by Lemma 1. This verifies the description of $Z(\mathrm{Mlt}(Q))$ and shows that $\mathrm{Inn}(Q)Z(\mathrm{Mlt}(Q)) = \{\psi \in \mathrm{Mlt}(Q);\ \psi(1) \in Z(Q)\}$. The latter group is also equal to $N_{\mathrm{Mlt}(Q)}(\mathrm{Inn}(Q))$, by Lemma 13. □

Nilpotency. Let $\mathcal{S}$ be a set of subsets of a set X. Suppose that $X \in \mathcal{S}$ and that $\mathcal{S}$ contains the least element, say I. Thus $I \subseteq X$ for each $X \in \mathcal{S}$. In the application below $X = Q$, Q a loop, and I is the trivial subloop, i.e. $I = \{1\}$.

Suppose that upon $\mathcal{S}$ there are defined two transformations, say α and β. Let both of them *respect inclusions*, i.e., if $S_1, S_1 \in \mathcal{S}$ and $S_1 \subseteq S_2$, then $\alpha(S_1) \subseteq \alpha(S_2)$ and $\beta(S_1) \subseteq \beta(S_2)$. Futhermore, let both of them be *monotonous*, with $\alpha(S) \supseteq S$ and $\beta(S) \subseteq S$, for every $S \in \mathcal{S}$.

Finally, let α and β be interconnected by

$$\beta\alpha(S) \subseteq S \text{ and } \alpha\beta(S) \supseteq S, \text{ for every } S \in \mathcal{S}.$$

In such a situation it is possible to build *lower series* $X \supseteq \beta(X) \supseteq \beta^2(X) \supseteq \dots$, and *upper series* $I \subseteq \alpha(I) \subseteq \alpha^2(I) \subseteq \dots$. It is well known that the lower series ends at I if and only if the upper series ends at X, and that, if the latter is true, then both series are of equal length. If the length is $n+1$, then n is the *nilpotency class* of $\mathcal{S}$ (with respect to α and β) and $\mathcal{S}$ is said to be *nilpotent*. Of course, if $\mathcal{S}$ is deterministically derived from an object $\mathcal{O}$, then the notions of nilpotency and nilpotency class are related to that object.

The objects in question now are loops, and the systems of subsets are the normal subloops of a loop Q. If $N \trianglelefteq Q$, then there obviously exists a unique $M \trianglelefteq Q$ such that $N \le M$ and $M/N = Z(Q/N)$. This is the operator α. The normal subloops $\alpha^i(1)$, $i \ge 0$, are the *iterated centers* $Z_i(Q)$, with $Z_1(Q) = Z(Q)$ and $Z_{i+1}(Q)/Z_i(Q) = Z(Q/Z_i(Q))$.

The inclusion $M = \alpha(N) \supseteq N$ follows from the fact that N/N is the trivial subgroup of Q/N. Hence $N/N \le Z(Q/N)$. Suppose now that $N_1 \le N_2$ are normal subloops of Q. Denote by π the homomorphism $Q/N_1 \to Q/N_2$, $xN_1 \mapsto xN_2$. If $M \trianglelefteq Q$ is such that $N_1 \le M$ and $M/N_1 \le Z(Q/N_1)$, then $\pi(M/N_1) \le Z(Q/N_2)$. Express $\pi(M/N_1)$ as L/N_2. Then $M \le L$. Setting $M = \alpha(N_1)$ yields $\alpha(N_1) \le \alpha(N_2)$.

Let us now show that for each $N \trianglelefteq Q$ there exists the least normal subloop $M \trianglelefteq Q$ such that $M \le N$ and $N/M \le Z(Q/M)$. The operator β is defined so that $\beta(N) = M$.

To verify the existence of M first note that $\mathrm{Mlt}(Q/N)$ coincides with the action of $\mathrm{Mlt}(Q)$ upon the cosets modulo N. Indeed, cosets are conjugate blocks, and hence $\mathrm{Mlt}(Q)$ acts upon them. Now, L_x sends yN upon $x(yN) = (xy)N = L_{xN}(yN)$. The action of L_x coincides with L_{xN}, and this is similarly true for every R_x. The coincidence is transferred to the multiplication groups since these groups are generated by the left and the right translations.

The fact that aN belongs to $Z(Q/N)$ thus means that each standard generator of $\mathrm{Inn}(Q)$ maps aN upon aN, by Theorem 24. If M_i, $i \in I$, are all $M_i \trianglelefteq Q$ such that $M_i \le N$ and $N/M_i \le Z(Q/M_i)$, then $M = \bigcap M_i$ is a normal subloop of Q. Each standard generator of $\mathrm{Inn}(Q)$ maps aM_i, $a \in N$, to aM_i, for every $i \in I$. Hence it maps $aM = a(\bigcap M_i) = \bigcap(aM_i)$ upon aM, which implies $N/M \le Z(Q/M)$.

The obvious inclusion $N/N \le Z(Q/N)$ implies $\beta(N) \le N$. Consider now normal subloops N_1 and N_2 such that $N_1 \le N_2$. Let $M \trianglelefteq Q$ be such that $N_2/M \le Z(Q/M)$. Consider $a \in N_1$ and $\varphi \in \mathrm{Inn}(Q)$. Then $\varphi(aM) = aM$ since $a \in N_2$ and $N_2/M \le Z(Q/M)$. Furthermore, $aN_1 = N_1$ and $\varphi(N_1) = N_1$, because $N_1 \trianglelefteq Q$. Hence $\varphi(a(M \cap N_1)) = a(M \cap N_1)$. Therefore $a(M \cap N_1) \in Z(Q/(N_1 \cap M))$, and thus $N_1/(M \cap N_1) \le Z(Q/(M \cap N_1))$. Setting $M = \beta(N_2)$ implies that $\beta(N_1) \le \beta(N_2) \cap N_1 \le \beta(N_2)$.

It remains to verify that $\beta\alpha(N) \le N$ and $\alpha\beta(N) \ge N$, for every $N \trianglelefteq Q$. If $M = \alpha(N)$, then $M/N = Z(Q/N)$. Hence $N \ge K$, where $K = \beta(M)$ is the least normal subloop such that $K \le M$ and $M/K \le Z(Q/K)$. Therefore $\beta\alpha(N) \le N$. To see $\alpha\beta(N) \ge N$, just note that $N/\beta(N) \le Z(Q/\beta(N))$.

This is why the first steps in the theory of nilpotent loops resemble those in the theory of nilpotent groups. A loop Q is thus *nilpotent of class k* if and only if $Z_k(Q) = Q$ and $k \ge 0$ is the least possible. Furthermore, each loop of nilpotency class 2 may be, up to isomorphism, expressed by an operation upon $G \times Z$, where both $(G, +)$ and $(Z, +)$ are abelian groups, and

$$(a, u) \cdot (b, v) = (a + b, u + v + \vartheta(a, b)) \text{ for all } u, v \in Z \text{ and } a, b \in G,$$

where $\vartheta \colon G \times G \to Z$ fulfils $\vartheta(0, a) = \vartheta(a, 0) = 0$, for all $a \in G$.

To see this consider a loop of nilpotency class two, and set $Z = Z(Q)$. From each coset modulo Z choose exactly one element. The chosen elements form a set, say G, and this set may be endowned with the structure of the factorloop Q/Z. The factorloop is an abelian group. The operation of G will thus be written additively. If $g_i \in G$ and $z_i \in Z$, $i \in \{1, 2\}$, then there exists $g_3 \in G$ and $z_3 \in Z$ such that $g_1 g_2 = g_3 z_3$. Note, that $(g_1 z_1)(g_2 z_2) = g_3(z_3 z_1 z_2)$ and that $g_3 = g_1 + g_2$. Denote z_3 by $\vartheta(g_1, g_2)$. This yields $g_1 z_1 \cdot g_2 z_2 = (g_1 + g_2)(\vartheta(g_1, g_2) z_1 z_2)$. Writing elements of Z additively thus shows that Q is isomorphic to a loop with operation

$$(g_1, z_1) \cdot (g_2, z_2) = (g_1 + g_2, \vartheta(g_1, g_2) + z_1 + z_2).$$

To get $(0, 0)$ as the neutral element of this loop it suffices to assume that the neutral element of Q is the element that is chosen from Z (which is also a coset). Such a choice also stipulates that $\vartheta(g, 0) = 0 = \vartheta(0, g)$ for all $g \in G$.

The definition of nilpotency by means of the operators α and β allows to introduce further concepts for which the term nilpotency may be used. These concepts are not discussed here. The nilpotency defined above is sometimes called *central nilpotency* in order to distinguish it from those other concepts.

Left and right nuclei. Let Q be a loop. By Lemma 23, $N_\lambda(Q)$ are the points fixed by $(\mathrm{RMlt}(Q))_1$, and $N_\rho(Q)$ are the points fixed by $(\mathrm{LMlt}(Q))_1$. A similar characterization in terms of the multiplication groups is as follows:

Proposition 25. *Let Q be a loop. Then*

(1) $\{L_a;\, a \in N_\lambda(Q)\} = C_{\mathrm{Mlt}(Q)}(\mathrm{RMlt}(Q)) = C_{\mathrm{Sym}(Q)}(\mathrm{RMlt}(Q))$, *and*

(2) $\{R_a;\ a \in N_\rho(Q)\} = C_{\mathrm{Mlt}(Q)}(\mathrm{LMlt}(Q)) = C_{\mathrm{Sym}(Q)}(\mathrm{LMlt}(Q))$.

Proof. If $a \in N_\lambda(Q)$ and $x, y \in Q$, then $L_aR_x(y) = a\cdot yx = ay\cdot x = R_xL_a(y)$. Hence $[L_a, R_x] = \mathrm{id}_Q$ if and only if $a \in N_\lambda(Q)$. If $\varphi \in (\mathrm{Sym}(Q))_1$ and $[L_a\varphi, R_x] = \mathrm{id}_Q$ for each $x \in Q$, then $a\varphi(yx) = a\varphi(y)\cdot x$ for all $x, y \in Q$. Setting $y = 1$ yields $L_a = L_a\varphi$. Thus $\varphi = \mathrm{id}_Q$. □

Proposition 26. *Let Q be a loop. If $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$, then $N_\lambda(Q) \trianglelefteq Q$. If $\mathrm{LMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$, then $N_\rho(Q) \trianglelefteq Q$.*

Proof. If $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$, then the centralizer of $\mathrm{RMlt}(Q)$ is also a normal subgroup of $\mathrm{Mlt}(Q)$. In such a case $N_\lambda(Q)$ is an orbit of a normal subgroup of $\mathrm{Mlt}(Q)$. The rest follows from Lemma 12 and Corollary 19. □

Proposition 27. *If Q is a left Bol loop, then $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$ and $N_\lambda(Q) \trianglelefteq Q$. If Q is a right Bol loop, then $\mathrm{LMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$ and $N_\rho(Q) \trianglelefteq Q$. If Q is a Moufang loop, then $N(Q) \trianglelefteq Q$ and both $\mathrm{LMlt}(Q)$ and $\mathrm{RMlt}(Q)$ are normal subgroups of $\mathrm{Mlt}(Q)$.*

Proof. By Proposition 26 it suffices to show that $\mathrm{RMlt}(Q) \trianglelefteq \mathrm{Mlt}(Q)$ if Q is left Bol, that is if $x(y\cdot xz) = (x\cdot yx)z$ for all $x, y, z \in Q$. The latter identity can be written as $L_xR_{xz} = R_zL_xR_x$. This means $L_x^{-1}R_zL_x = R_{xz}R_x^{-1}$. Nothing more is needed since Q is a LIP loop and $\mathrm{RMlt}(Q)$ is generated by the right translations R_x, $x \in Q$. □

Transversals. Let $H \leq G$ be groups. A pair (A, B) of subsets of G is said to form H*-connected* transversals if A is a left transversal to H in G, B is a right transversal to H in G, and $[a, b] \in H$ for all $(a, b) \in A \times B$.

Lemma 28. *Let Q be a loop. Put $G = \mathrm{Mlt}(Q)$ and $H = \mathrm{Inn}(Q)$. Furthermore, set $A = \{L_x;\ x \in Q\}$ and $B = \{R_x;\ x \in Q\}$. Then (A, B) forms H-connected transversals, $\langle A, B\rangle = G$, and the core of H in G is trivial.*

Proof. As follows from Lemma 14 both A and B are both-sided transversals of H to G. The core of H in G is trivial by Lemma 15. Finally, $L_xR_y(1) = R_yL_x(1) = xy$ for all $x, y \in Q$. □

There seems to be nothing remarkable in Lemma 28. The point is that the statement may be reversed. The proof is not long, but will not be included. We have:

Theorem 29. *Let G and H be groups, and A and B subsets of G such that $H \leq G$, (A, B) forms H-connected transversals, $\langle A, B\rangle = G$, and the core of H in G is trivial. Then there exists a loop Q such that $G = \mathrm{Mlt}(Q)$, $H = \mathrm{Inn}(Q)$, $A = \{L_x;\ x \in Q\}$ and $B = \{R_x;\ x \in Q\}$.*