SOME INTRODUCTORY FACTS ON LOOPS AND QUASIGROUPS

ALEŠ DRÁPAL

1. Definitions and some basic facts

Let $\cdot$ be a binary operation upon a set Q. For each $a \in Q$ define the *left translation* $L_a\colon Q \to Q$, $x \mapsto ax$. Similarly, $R_a\colon Q \to Q$, $x \mapsto xa$, is the *right translation* of Q.

Say that $(Q, \cdot)$ is a *quasigroup* if all L_a and R_a, $a \in Q$, are permutations of Q (i.e., $L_a, R_a \in S_Q$, where S_Q is the symmetric group upon Q).

If Q is a quasigroup, then the equations $ax = b$ and $ya = b$ have unique solutions x and y for all $a, b \in Q$. This can be used as an alternative definition of a quasigroup.

Let Q be a quasigroup, and assume $a, b \in Q$. Set $x = a\backslash b$ if $ax = b$, and $y = b/a$ if $ya = b$. Now, $\backslash$ and $/$ are binary operations on Q. It is easy to see that

$$x(x\backslash y) = y = x\backslash(xy) \quad \text{and} \quad (y/x)x = y = (yx)/x \tag{1.1}$$

for all $x, y \in Q$. On the other hand, it is also easy to see that if upon a set Q there are defined binary operations $\cdot$, $\backslash$ and $/$ that satisfy (1.1), then $(Q, \cdot)$ is a quasigroup, and

$$x/(y\backslash x) = y = (x/y)\backslash x \tag{1.2}$$

for all $x, y \in Q$, since $x/(y\backslash x) = (y \cdot (y\backslash x))/(y\backslash x) = y$.

A quasigroup Q is a loop if it possesses a neutral element, i.e. an element $1 \in Q$ such that $x1 = x = 1x$ for all $x \in Q$. Clearly $x/1 = x = 1\backslash x$.

Note that every quasigroup is *cancellative*, i.e. if $ax = bx$ or $xa = xb$, then $a = b$. This property means that left and right translations are injective. If Q is finite, then this suffices for $(Q, \cdot)$ to be a quasigroup.

1.1. **The multiplication group and congruences.**

Let Q be a quasigroup. The permutation group $\langle L_x;\ x \in Q\rangle$ is called the *left multiplication group* of Q. The right translations generate the *right multiplication group.* Furthermore, $\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q\rangle$ is called the *multiplication group* of Q.

If G is a permutation group upon a set Ω and $\omega \in \Omega$, then $G_\omega = \{g \in G;\ g(\omega) = \omega\}$ is a subgroup of G, the *stabilizer* of G at ω.

If Q is a loop, then $(\mathrm{Mlt}(Q))_1$ is known as the *inner mapping group*, and is usually denoted by $\mathrm{Inn}(Q)$.

Let G be a transitive permutation group upon Ω, $\omega \in \Omega$, and for each $\alpha \in \Omega$ let $t_\alpha \in G$ be such that $t_\alpha(\omega) = \alpha$. Assume that $t_\omega = \mathrm{id}_\Omega$ and that $G = \langle X\rangle$. It is well known that then $G_\omega = \langle t^{-1}_{x(\alpha)} x t_\alpha;\ x \in X \text{ and } \alpha \in \Omega\rangle$.

Proposition 1.1. *Let Q be a loop. Then* $\mathrm{Inn}(Q) = \langle L^{-1}_{xy} L_x L_y, R^{-1}_{yx} R_x R_y, R^{-1}_x L_x\rangle$.

Proof. Put $G = \mathrm{Mlt}(Q)$ and note that $L_y(1) = y$ for every $y \in Q$. Therefore the set of all $L_{xy}^{-1}L_xL_y$ and $L_{yx}^{-1}R_xL_y$ 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 $L_{yx}^{-1} = (R_{yx}^{-1}L_{yx})^{-1}R_{yx}^{-1}$. □

An equivalence $\sim$ is a congruence of a quasigroup Q if and only if it is compatible with all the three operations, i.e. with $\cdot$, $\backslash$ and $/$. This can be slightly simplified:

Lemma 1.2. *Let $\sim$ be an equivalence upon Q, Q a quasigroup. Then $\sim$ is a congruence of Q if the following implication is true for all $u, v, x \in Q$:*

$$u \sim v \quad \Rightarrow \quad ux \sim vx,\ xu \sim xv,\ u/x \sim v/x \text{ and } x\backslash u \sim x\backslash v. \tag{1.3}$$

Proof. What is needed is to prove that if (1.3) holds for all $u, v, x \in Q$, and $u \sim v$, then $x/u \sim x/v$ and $u\backslash x \sim v\backslash x$. By (1.2), $u = x/(u\backslash x) \sim v$. Hence $x \sim v(u\backslash x)$ and $v\backslash x \sim u\backslash x$. The case $x/u \sim x/v$ is mirror symmetric. □

Let G be permutation group upon Ω. A set $\Gamma \subseteq \Omega$ is called a *block* of G if $\Gamma \neq \emptyset$, and

$$\forall\, \alpha, \beta \in \Gamma \text{ and } \forall g \in G\ (g(\alpha) \in \Gamma \ \Rightarrow\ g(\beta) \in \Gamma). \tag{1.4}$$

It is easy to see that if Γ is a block, and $g \in G$, then either $g(\Gamma) = \Gamma$ or $g(\Gamma) \cap \Gamma = \emptyset$. Furthermore, $g(\Gamma)$ is also a block—all such blocks are called *conjugates* of Γ. If G is transitive, then a complete set of conjugate blocks partitions Ω. Each block thus induces an equivalence upon Ω, if G is transitive. If such an equivalence is denoted by $\sim$, then it fulfils $\alpha \sim \beta \Rightarrow g(\alpha) \sim g(\beta)$ for all $\alpha, \beta \in \Omega$ and $g \in G$. On the other hand, if $\sim$ satisfies this condition, then each block of $\sim$ is a block of G.

Proposition 1.3. *Let Q be quasigroup. Then $S \subseteq Q$ is a block of* $\mathrm{Mlt}(Q)$ *if and only if it is a block of a congruence of Q.*

Proof. Note that $L_x^{-1}(u) = x\backslash u$ and $R_x^{-1}(u) = u/x$. Thus, by Lemma 1.2, $\sim$ is a congruence of Q if and only if $u \sim v$ implies $\psi(u) \sim \psi(v)$ for all $u, v \in Q$ and $\psi \in \mathrm{Mlt}(Q)$. □

If Q is a loop and $\sim$ a congruence of loop, then $N = [1]_\sim$ is a subloop of Q. Indeed $x \sim 1$ and $y \sim 1$ imply $xy \sim 1 \cdot 1 = 1$, $x/y \sim 1/1 = 1$ and $x\backslash y \sim 1\backslash 1 = 1$. A subloop of a loop is called *normal* if it is a block of a congruence.

Theorem 1.4. *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 $L_{xy}^{-1}L_xL_y(N) = N$, $R_{yx}^{-1}R_xR_y(N) = N$ and $R_x^{-1}L_x(N) = N$. In view of Proposition 1.1 this means that (iii) ⇔ (iv).

It remains to prove (iii) ⇒ (i). Each element of $\mathrm{Mlt}(Q)$ can be written as $L_x\varphi$, where $\varphi \in \mathrm{Inn}(Q)$ and $x \in Q$. 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 $\mathrm{Mlt}(Q)$. □

1.2. **Isotopy, inverse property, nucleus.** Suppose that Q_1 and Q_2 are quasigroups. A triple (α, β, γ) is said to be an *isotopism* $Q_1 \to Q_2$ if each of α, β and γ is a bijection $Q_1 \to Q_2$, and

$$\alpha(x)\beta(y) = \gamma(xy) \text{ for all } x, y \in Q_1. \tag{1.5}$$

If $(\alpha_1, \beta_1, \gamma_1)\colon Q_1 \to Q_2$ and $(\alpha_2, \beta_2, \gamma_2)\colon Q_2 \to Q_3$ are isotopisms, then the composition $(\alpha_2\alpha_1, \beta_2\beta_1, \gamma_2\gamma_1)$ is an isotopism $Q_1 \to Q_3$. This is clear, and it is also clear that $(\alpha_1^{-1}, \beta_1^{-1}, \gamma_1^{-1})$ is an isotopism $Q_2 \to Q_1$.

An isotopism $Q \to Q$ is called an *autotopism.* By the observations above, all autotopisms of Q form a group. This group will be denoted by $\mathrm{Atp}(Q)$.

Lemma 1.5. *Let Q be a loop, and let $(\alpha, \beta, \gamma) \in \mathrm{Atp}(Q)$. Put $a = \alpha(1)$ and $b = \beta(1)$.*

(i) *If $a = 1$, then $\beta = \gamma = R_b\alpha$; and*
(ii) *If $b = 1$, then $\alpha = \gamma = L_a\beta$.*

Proof. Assume $a = 1$. By (1.5), $\beta(y) = \alpha(1)\beta(y) = \gamma(1y) = \gamma(y)$, for each $y \in Q$. Furthermore, $\alpha(x)b = \beta(x)$ for each $x \in Q$. □

For a loop Q put $N_\lambda(Q) = \{a \in Q;\ a(xy) = (ax)y$ for all $x, y \in Q$, and call it the *left nucleus* of Q. The *right nucleus* $N_\rho(Q)$ consists of all $a \in Q$ such that $(xy)a = x(ya)$ for all $x, y \in Q$.

Lemma 1.6. *Let Q be a loop, and let $\alpha, \beta, \gamma \in S_Q$.*

(i) $(\mathrm{id}_Q, \beta, \gamma) \in \mathrm{Atp}(Q)$ *if and only if there exists $b \in N_\rho(Q)$ such that $\beta = \gamma = R_b$.*
(ii) $(\alpha, \mathrm{id}_Q, \gamma) \in \mathrm{Atp}(Q)$ *if and only if there exists $a \in N_\lambda(Q)$ such that $\alpha = \gamma = L_a$.*

An element $a \in Q$ is said to satisfy the *left inverse property* (LIP) if there exists $b \in Q$ such that $L_a^{-1} = L_b$. The latter fact can be expressed both as $a(bx) = x$ or $b(ax) = x$, $x \in Q$. Hence $b = 1/a = a\backslash 1$. If a satisfies the LIP, then it is therefore usual to write $1/a = a\backslash 1$ as a^{-1}.

It is also usual to say that a is an *LIP element*, instead of saying that a satisfies the LIP. Note that the LIP can be succinctly expressed as $L_a^{-1} = L_{a^{-1}}$. Similarly, the mirror notion of RIP can be expressed as $R_a^{-1} = R_{a^{-1}}$.

Lemma 1.7. *Let Q be a loop. If $a \in N_\lambda(Q)$, then a is an LIP element. If $a \in N_\rho(Q)$, then a is an RIP element.*

Proof. Indeed, $a((a\backslash 1)x) = (a(a\backslash 1))x = x$ for every $a \in N_\lambda(Q)$ and $x \in Q$. If $a \in N_\rho(\mu)$, then $(x(1/a))a = x((1/a)a) = x$. □

Let Q be a quasigroup and S a set. Suppose that α, β and γ are bijections $Q \to S$. Then there clearly exists just one quasigroup operation upon S such that (α, β, γ) is an isotopism $Q \to S$. This operation can be described by formula $\gamma(\alpha^{-1}(x)\beta^{-1}(y))$. We shall call it the *quasigroup induced* by (α, β, γ).

Let Q be a quasigroup, and let $\alpha, \beta \in S_Q$. Then $x * y = \alpha^{-1}(x)\beta^{-1}(y)$ defines a strucure of another quasigroup upon Q. This quasigroup is induced by $(\alpha, \beta, \mathrm{id}_Q)$. Every such quasigroup is called a *principal isotope* of Q.

Suppose the principal isotope $x * y = \alpha^{-1}(x)\beta^{-1}(y)$ of a quasigroup Q is a loop, with u the unit. Put $f = \beta^{-1}(u)$ and $e = \alpha^{-1}(u)$. Then $\alpha(x) = \alpha(x) * u = xf = R_f(x)$, and $\beta(y) = L_e(y)$, for all $x, y \in Q$. Hence $x * y = (x/f)(e\backslash y)$.

Proposition 1.8. *A principal isotope of a quasigroup Q is a loop if and only if there exist $e, f \in Q$ such that the operation of the isotope can be expressed as $x * y = (x/f)(e\backslash y)$, for all $x, y \in Q$.*

Proof. We have already observed that there must exist $e, f \in Q$ such that $x * y = (x/f)(e\backslash y)$ for all $x, y \in Q$. If the operation $*$ is determined in such a way, then it is a loop since ef is its unit. □

Let $(\alpha, \beta, \gamma)\colon Q_1 \to Q_2$ be an isotopism of quasigroups. Define a new loop Q_3 so that $\gamma\colon Q_3 \cong Q_2$. Note that Q_1 and Q_3 share the same underlying set. Now, Q_3 has to be a principal isotope of Q_1 since

$$(\alpha, \beta, \gamma) = (\gamma, \gamma, \gamma)(\gamma^{-1}\alpha, \gamma^{-1}\beta, \mathrm{id}_{Q_1}).$$

In view of Proposition 1.8 we can thus immediately state:

Theorem 1.9. *Let Q be a quasigroup. Each quasigroup isotopic to Q is isomorphic to one of its principal isotopes. For each loop isotopic to Q there exist $e, f \in Q$ such that the loop is isomorphic to the loop $Q(*)$, $x * y = (x/f)(e\backslash y)$ for all $x, y \in Q$.*

Let Q be a loop. An element $x \in Q$ is said to satisfy the *inverse property* (IP) if satisfies both the LIP and the RIP. Such elements are also known as *IP elements.*

The *middle nucleus* $N_\mu(Q)$ of a loop Q is defined as $\{a \in Q;\ x(ay) = (xa)y$ for all $x, y \in Q\}$. The intersection $N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$ is known as the *nucleus* of Q, and is denoted by $N(Q)$.

Lemma 1.10. *Let Q be a loop. Each $a \in N_\mu(Q)$ is an IP element, $b = a^{-1} \in N_\mu(Q)$ and $(R_b, L_a, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$. On the other hand, if $(\alpha, \beta, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$, then there exist $a, b \in N_\mu(Q)$ such that $b = a^{-1}$, $\alpha = R_b$ and $\beta = L_a$.*

Proof. Let a be an element of the middle nucleus. Put $b = a\backslash 1$. Then $(xa)b = x(ab) = x$. Hence a is an RIP element, and $b = a^{-1}$. Now, a is a also an LIP element, by mirror argument. Consider $(xb)y$ and write x as za. Then $(xb)y = (za \cdot b)y = zy$ and $x(by) = (za)(by) = z(a(by)) = zy$, since a is an LIP element. Thus $b \in N_\mu(Q)$, and hence $(xb)(ay) = xy$ for all $x, y \in Q$. The latter fact means that $(R_b, L_a, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$.

Suppose that $(\alpha, \beta, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$. Then $(\alpha^{-1}, \beta^{-1}, \mathrm{id}_Q) \in \mathrm{Atp}(Q)$, and by Proposition 1.8 there exist $a, b \in Q$ such that $\alpha = R_b$ and $\beta = L_a$. Thus $(xb)(ay) = xy$ for all $x, y \in Q$. Setting $x = 1$ and $y = 1$ implies that a and b are IP elements, $b = a^{-1}$. Thus $(xb)(ay) = xy = ((xb)a)y$ for all $x, y \in Q$ since $(xb)a = x$. Setting $z = xb$ yields $z(ay) = (za)y$, and so $a \in N_\mu$. □

1.3. **Closure conditions on translations and loop laws.** Let Q be a loop. Put $L = \{L_x;\ x \in Q\}$. Say that L is closed under

- *inverses* if $\psi^{-1} \in L$ for every $\psi \in L$;
- *compositions* if $\varphi\psi \in L$ for all $\varphi, \psi \in L$;
- *conjugations* if $\varphi\psi\varphi^{-1} \in L$ for all $\varphi, \psi \in L$; and
- *twists* if $\varphi\psi\varphi \in L$ for all $\varphi, \psi \in L$.

Similar conditions can be stated for $R = \{R_x;\ x \in Q\}$.

It is clear that L is closed under inverses if and only if every element of Q is an LIP element. Such loops are called LIP loops. In such a loop $1/x = x\backslash 1 = x^{-1}$ for each $x \in Q$, $(x^{-1})^{-1} = x$ and $x^{-1}(xy) = y$, for all $x, y \in Q$.

RIP loops are defined in a mirror way. A loop is an IP loop if it is both an LIP loop and an RIP loop. A loop Q is said to have the *antiautomorphic inverse property* if $1/x = x\backslash 1$ for all $x \in Q$ and $(xy)^{-1} = y^{-1}x^{-1}$ for all $x, y \in Q$. Instead of saying that Q has such a property it is usual to say that Q is an AAIP loop.

Lemma 1.11. *Each IP loop is also an AAIP loop.*

Proof. Let Q be an IP loop, and $x, y \in Q$. Then $y(xy)^{-1} = (x^{-1}(xy))(xy)^{-1} = x^{-1}$, and so $(xy)^{-1} = y^{-1}x^{-1}$. □

If L is *closed under compositions*, then for all $a, b \in Q$ there exists $c \in Q$ such that $L_aL_b = L_c$. This implies $c = L_c(1) = L_aL_b(1) = ab$. However, the equality $L_aL_b = L_{ab}$ is just a form of the associative law. Hence L is closed under compositions if and only if Q is a group.

If L is *closed under conjugations*, then for all $a, b \in Q$ there exists $c \in Q$ such that $L_aL_bL_a^{-1} = L_c$. Then $L_aL_b = L_cL_a$, and $ab = ca$. Thus $c = (ab)/a$. Hence L is closed under conjugation if and only if $a(b(a\backslash x)) = ((ab)/a)x$ for all $a, b, x \in Q$.

Loops satisfying the law $x(y(x\backslash z)) = ((xy)/x)z$ are called *left conjugacy closed* (LCC). The RCC lops are those that satisfy $((z/x)y)x = z(x\backslash(yx))$. The *conjugacy closed* loops (CC) are the loops that are both LCC and RCC.

If L is *closed under twists*, then for all $a, b \in Q$ there exists $c \in Q$ such that $L_aL_bL_a = L_c$. Clearly, $c = a(ba)$. Hence L is closed under twists if and only if Q satisfies the law $x(y(xz)) = (x(yx))z$. This is known as the *left Bol*, and the loops that satisfy this law are called left Bol loops. The *right Bol* loops satisfy $((zx)y)x = z((xy)x)$. Loops that are both left Bol and right Bol are called *Moufang.*

The variety of Moufang loops can be described by a single law. While it will not be proved here, it is true that the variety of loops is the variety of Moufang loops if and only if it is given by any (and thus all) of the following three identities:

$$x(y(xz)) = ((xy)x))z, \quad ((zx)y)x = z(x(yx)) \text{ and } (xy)(zx) = x((yz)x). \tag{1.6}$$

2. Nucleus, center and the nilpotency

Proposition 2.1. *Let Q be a loop. Then each of $N_\lambda(Q)$, $N_\mu(Q)$, $N_\rho(Q)$ and $N(Q)$ is a group that is a subloop of Q.*

Proof. Because of mirror symmetry it suffices to prove only the cases of $N_\lambda(Q)$ and $N_\mu(Q)$. Let $a, b \in N_\lambda(Q)$. By Lemma 1.6, $(L_a^{-1}, \mathrm{id}_Q, L_a^{-1})$ is equal to some $(L_c, \mathrm{id}_Q, L_c)$, $c \in N_\lambda(Q)$. Clearly, $c = a\backslash 1$. By Lemma 1.7, $a^{-1} \in N_\lambda(Q)$. By Lemma 1.6, $(L_aL_b, \mathrm{id}_Q, L_aL_b) = (L_{ab}, \mathrm{id}_Q, L_{ab}) \in \mathrm{Atp}(Q)$, and $ab \in N_\lambda(Q)$. Since a is a LIP element, $a\backslash b = a^{-1}b \in N_\lambda(Q)$ too. There is also $a/b \in N_\lambda(Q)$, since $a/b = ab^{-1}$, by $(ab^{-1})b = a(b^{-1}b) = a$.

Suppose now that $a, b \in N_\mu(Q)$. By Lemma 1.10, a and b are IP elements, with $a^{-1}, b^{-1} \in N_\mu(Q)$. Hence $a/b = ab^{-1}$, $a\backslash b = a^{-1}b$, and so the only remaining step is to show that $ab \in N_\mu(Q)$. If $x, y \in Q$, then $(x(ab))y = ((xa)b)y = (xa)(by) = x(a(by)) = x((ab)y)$. □

For a loop Q put $C(Q) = \{a \in Q;\ ax = xa \text{ for all } x \in Q\}$, and $Z(Q) = C(Q) \cap N(Q)$. Call $Z(Q)$ the *center* of Q.

Lemma 2.2. *Let Q be a loop, and let z be an element of Q. Then $z \in Z(Q)$ if and only if $\varphi(z) = z$ for every $\varphi \in \mathrm{Inn}(Q)$.*

Proof. Note that $z \in N_\lambda(Q)$ if and only if z is fixed by every $R_{yx}^{-1}R_xR_y$, $z \in N_\rho(Q)$ if and only if z is fixed by every $L_{xy}^{-1}L_xL_y$, and $z \in C(Q)$ if and only if z is fixed by every $R_x^{-1}L_x$. Thus, by Proposition 1.1, z is fixed by every $\varphi \in \mathrm{Inn}(Q)$ if and only if $z \in N_\lambda(Q) \cap N_\rho(Q) \cap C(Q)$. It remains to prove that such z belongs to $N_\mu(Q)$ as well. However, that is easy, since for every such z and every $x, y \in Q$ it is true that $x(zy) = x(yz) = (xy)z = z(xy) = (zx)y = (xz)y$. □

Note that Lemma 2.2 can be also expressed as the first equivalence in

$$z \in Z(Q) \quad \Leftrightarrow \quad (\mathrm{Mlt}(Q))_z \supseteq \mathrm{Inn}(Q) \quad \Leftrightarrow \quad (\mathrm{Mlt}(Q))_z = \mathrm{Inn}(Q). \tag{2.1}$$

For the second equivalence consider $\psi \in (\mathrm{Mlt}(Q))_z$ and express it as $L_a\varphi$, $\varphi \in \mathrm{Inn}(Q)$. Then $z = \psi(z) = L_a(z) = az$, which implies $a = 1$.

If G is permutation group upon a set Ω, and $\omega \in \Omega$, then the set $\{\alpha \in \Omega;\ G_\alpha = G_\omega\}$ is always a block of G. Furthermore, the normalizer $N_G(G_\omega)$ can be expressed as $\{g \in G;\ G_{g(\omega)} = G_\omega\}$. These well known fact will be used in the following statement.

Theorem 2.3. *Let Q be a loop. Then $Z(Q)$ is a normal subloop of Q, $Z(\mathrm{Mlt}(Q)) = \{L_z;\ z \in Z(Q)\}$ and $N_{\mathrm{Mlt}(Q)}(\mathrm{Inn}(Q)) = Z(\mathrm{Mlt}(Q))\,\mathrm{Inn}(Q)$.*

Proof. By (2.1), $Z(Q)$ is a block of $\mathrm{Mlt}(Q)$. By Proposition 1.3 it is a normal subloop of Q. Each element of $\mathrm{Mlt}(Q)$ can be uniquely expressed as $L_x\varphi$, $\varphi \in \mathrm{Inn}(Q)$ and $x \in Q$. If this element centralizes each R_y, then $x\varphi(y) = L_x\varphi R_y(1) = R_yL_x\varphi(1) = xy$. This implies $\varphi = \mathrm{id}_Q$. Hence each element of $Z(\mathrm{Mlt}(Q))$ is equal to some L_z, $z \in Q$. Now, $L_zL_x = L_xL_z$ means that $z(xy) = x(zy)$, which gives $z \in C(Q)$ and $z \in N_\rho(Q)$. Furthermore, $L_zR_x = R_xL_z$ yields $z(yx) = (zy)x$, which means that $z \in N_\lambda(Q)$. Then $z \in N_\mu(Q)$ as well, as proved in the last part of the proof of Lemma 2.2. □

Let Q be a loop. Define *iterated centers* $Z_i(G)$, $i \geq 0$, as normal subloops of Q such that $Z_0(Q) = 1$ and $Z_{i+1}(Q)/Z_i(Q) = Z\big(Q/Z_i(Q)\big)$. Call Q *nilpotent* if $Z_s(Q) = Q$ for some $s \geq 0$. The least such s is called the *nilpotency degree* of the (nilpotent) loop Q.

The nilpotent loops behave similarly as nilpotent groups. This will be elaborated in a future version of this text.

3. Medial quasigroups

A good illustration of the strength of autotopisms is a proof of the Toyoda theorem given below. Toyoda theorem is concerned with medial quasigroups, i.e. quasigroups Q such that

$$(xy)(uv) = (xu)(yv) \ \text{ for all } \ x, y \in Q. \tag{3.1}$$

Law (3.1) is called *medial.* However, some authors prefer to call it *entropic.* It is easy to verify that if G is an abelian group, $c \in G$, and $\varphi, \psi \in \mathrm{Aut}(G)$ commute, then the formula

$$x * y = \varphi(x) + \psi(y) + c \ \text{ for all } \ x, y \in G \tag{3.2}$$

describes a medial quasigroup $(G, *)$. Toyoda theorem states the converse:

Theorem 3.1. *Let $*$ be a quasigroup operation upon a set G. Suppose that $*$ satisfies the medial law (3.1). Then upon G there can be defined an abelian group with operation $+$ such that (3.2) holds for some $c \in G$ and $\varphi, \psi \in \operatorname{Aut}(G(+))$, where $\varphi\psi = \psi\varphi$.*

Proof. Consider a principal isotope of $*$ that is a loop. The existence of such an isotope follows from Proposition 1.8. Therefore upon G there exists a loop Q with operation $\cdot$, and $\alpha, \beta \in S_G$ such that $x * y = \alpha(x)\beta(y)$. The medial law can thus be expressed as

$$\alpha\big(\alpha(x)\beta(y)\big) \cdot \beta\big(\alpha(u)\beta(v)\big) = \alpha\big(\alpha(x)\beta(u)\big) \cdot \beta\big(\alpha(y)\beta(v)\big),$$

and that is equivalent to

$$\alpha\big(x\beta\alpha^{-1}(u)\big) \cdot \beta\big(\alpha(y)v\big) = \alpha\big(x\beta(y)\big) \cdot \beta(uv).$$

The latter equality means that

$$(\alpha L_x \beta\alpha^{-1}, \beta L_{\alpha(y)}, L_{\alpha(x\beta(y))}\beta) \in \operatorname{Atp}(Q) \text{ for all } x, y \in G.$$

Hence also

$$(\alpha\beta^{-1}L_x^{-1}\alpha^{-1}, L_{\alpha(z)}^{-1}\beta^{-1}, \beta^{-1}L_{\alpha(x\beta(z))}^{-1}) \in \operatorname{Atp}(Q) \text{ for all } x, z \in G.$$

By composing the two autotopisms we get that

$$(\mathrm{id}_G, \beta L_{\alpha(y)}L_{\alpha(z)}^{-1}\beta^{-1}, L_{\alpha(x\beta(y))}L_{\alpha(x\beta(z))}^{-1}) \in \operatorname{Atp}(Q) \tag{3.3}$$

for all $x, y, z \in Q$. Fix $x = x_0$ and choose $z = z_0$ in such a way that $\alpha(x_0\beta(z_0)) = 1$. By (3.3) and Lemma 1.6, $\alpha(x_0\beta(y)) \in N_\rho(Q)$ for every $y \in Q$. However, that means that every element of Q is in the right nucleus, and so Q is a group, i.e. the operation $\cdot$ is associative.

From Lemma 1.6 and (3.3) it also follows that for all $u \in Q$ there exists $v \in Q$ so that $\beta L_u \beta^{-1} = L_v$. This means that $\beta(ux) = v\beta(x)$ for all $x \in Q$. Setting $b = \beta(1)$ and $x = 1$ yields $v = \beta(u)b^{-1}$. Hence $\beta(xy) = \beta(x)b^{-1}\beta(y)$ for all $x, y \in Q$. Writing this as $\beta(xy)b^{-1} = \beta(x)b^{-1}\beta(y)^{-1}b^{-1}$ implies that $\psi\colon x \mapsto \beta(x)b^{-1}$ is an automorphims of Q, and that $\beta(x) = \psi(x)b$ for all $x \in Q$.

Making a mirror argument (i.e. using the fact that the quaisgroup opposite to $*$ is medial, and its operation can be expressed as $\alpha(y)\beta(x) = \beta(x) \circ \alpha(y)$, where $\circ$ is the operation of the opposite loop Q^{op}) implies that there exist $a \in Q$ and $\varphi \in \operatorname{Aut}(Q)$ such that $\alpha(y) = \varphi(y) \circ a = a\varphi(y)$ for all $y \in Q$.

By Lemma 1.6 and (3.3), the value of

$$\alpha(x\beta(y))\alpha(x\beta(z))^{-1} = a\varphi(x)\varphi\beta(y)\varphi\beta(z)^{-1}\varphi(x)^{-1}a^{-1} = a\varphi(x\beta(y)\beta(z)^{-1}x^{-1})a^{-1} \tag{3.4}$$

depends only upon y and z. Thus x commutes with every $\beta(y)\beta(z)^{-1}$, and that makes Q a commutative group. The value of (3.4) is equal to $\varphi(\beta(y)\beta(z)^{-1}) = \varphi(\psi(yz^{-1}))$.

Now, $\beta L_{\alpha(y)}L_{\alpha(z)}^{-1}\beta^{-1} = \psi(L_{\alpha(y)(\alpha(z))^{-1}})\psi^{-1} = L_{\psi\varphi(yz^{-1})}$. Using (3.3) and Lemma 1.6 once more yields $\varphi(\psi(yz^{-1})) = \psi\varphi(yz^{-1})$ for all $y, z \in Q$. Thus $\varphi\psi = \psi\varphi$ and $x * y = \varphi(x) \cdot \psi(y) \cdot (ab)$ for all $x, y \in Q$. □