It is immediate to observe that each loop of order 2 is isomorphic to $(\mathbb{Z}_2, +)$ and that each loop of order 3 is isomorphic to $(\mathbb{Z}_3, +)$.

Theorem. *Each loop of order ≤ 4 is a group.*

Proof. What remains is the order 4. Let Q be a 4-element loop with unit e. Suppose first that $x^2 = e$ for all $x \in Q$. Assume that $Q = \{0, 1, 2, 3\}$ and $e = 0$. The table upon the left may be completed in only one way to a latin square (on the right). The multiplication table upon the right describes a group that is isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

	0	1	2	3
0	0	1	2	3
1	1	0		
2	2		0	
3	3			0

→

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Assume now that there exists $x \neq e$ such that $x^2 = y \neq e$. The elements e, x and y are pairwise distinct. Assume that $e = 0$, $x = 1$, $y = 2$ and verify the completion to $(\mathbb{Z}_4, +)$ below (the first cell to fill is $(3, 3)$).

	0	1	2	3
0	0	1	2	3
1	1	2		
2	2			
3	3			

→

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

□

Lemma 1. *Let Q be a loop of order 5. If the mapping $x \mapsto x^2$ is a permutation of Q, then $Q \cong (\mathbb{Z}_5, +)$.*

Proof. Put $Q_1 = Q \setminus \{1\}$. Then $x \mapsto x^2$ permutes Q_1 and this permutations lacks a fixed point. The permutation has one or two cycles. In the former case let us assume that the permutation is equal to $(a\,b\,c\,d)$. In the latter case let it be $(a\,b)(c\,d)$. In the former case there is only one completion to a latin square (first positions to fill are (a, d) and (d, a)):

	1	a	b	c	d
1	1	a	b	c	d
a	a	b			
b	b		c		
c	c			d	
d	d				a

→

	1	a	b	c	d
1	1	a	b	c	d
a	a	b	d	1	c
b	b	d	c	a	1
c	c	1	a	d	b
d	d	c	1	b	a

Let us now consider the case of $(a\,b)(c\,d)$.

	1	a	b	c	d
1	1	a	b	c	d
a	a	b			
b	b		a		
c	c			d	
d	d				c

The table upon the right cannot be completed to a latin square since the only positions to place the four entries a and b into rows c and d are (c, d) and (d, c).

This shows that up to isomorphism there is only one loop Q of order 5 such that $x \mapsto x^2$ permutes Q. The group $(\mathbb{Z}_5, +)$ fulfils this requirement. □

Lemma 2. *Up to isomorphism there is only one loop Q of order 5 in which $x \mapsto x^2$ does not permute Q and in which there exists no $x \neq 1$ such that $x^2 = 1$.*

Proof. Let Q be such a loop. There exist $a, b, s \in Q$ such that $a^2 = b^2 = s \neq 1$ and $a \neq b$. Therefore there exists $c \in Q$ such that $Q = \{1, a, b, c, s\}$. This yields a partial table in which the only row that does not carry s is the row c and the only column that does not carry s is the column c. Hence $c^2 = s$.

There has to be $s^2 \in \{a, b, c\}$. Let us assume that $s^2 = a$. If $as = 1$, then (a, b) and (a, c) are the only unfilled entries in the row a, implying $ab = c$ and $ac = b$. That means $\{b, c\} \cap \{sb, sc\} = \emptyset$. Hence $sx \in \{b, c\}$ may happen if and only if $x = a$. That is impossible. Therefore $as \neq 1$.

There thus exists $x \in \{b, c\}$ such that $ax = 1$. With no loss of generality it may be assumed that $x = b$. The rest can be completed uniquely, see below:

$$\begin{array}{c|ccccc} & 1 & a & b & c & s \\ \hline 1 & 1 & a & b & c & s \\ a & a & s & 1 & & \\ b & b & & s & & \\ c & c & & & s & \\ s & s & & & & a \end{array} \quad \to \quad \begin{array}{c|ccccc} & 1 & a & b & c & s \\ \hline 1 & 1 & a & b & c & s \\ a & a & s & 1 & b & c \\ b & b & c & s & a & 1 \\ c & c & 1 & a & s & b \\ s & s & b & c & 1 & a \end{array} \tag{L5.1}$$

□

To finish the classification of loops of order 5 it may be thus assumed that there exists $a \in Q$ such that $a^2 = 1$ and $a \neq 1$. Put $X = Q \setminus \{1, a\}$. Since both L_a and R_a switch 1 and a, both of them act upon X. Denote $L_a \restriction X$ by σ and $R_a \restriction X$ by $\bar{\sigma}$. With no loss of generality it may be assumed that $X = \{b, c, d\}$ and $\sigma = (b\,c\,d)$. Note that $\bar{\sigma}$ is either σ or σ^{-1}.

Lemma 3. *Up to isomorphism there is only one loop Q of order 5 in which there exist at least three $x \in Q$ such that $x^2 = 1$.*

Proof. This follows from the comments above and from the unique completion below.

$$\begin{array}{c|ccccc} & 1 & a & b & c & d \\ \hline 1 & 1 & a & b & c & d \\ a & a & 1 & c & d & b \\ b & b & & 1 & & \\ c & c & & & & \\ d & d & & & & \end{array} \quad \to \quad \begin{array}{c|ccccc} & 1 & a & b & c & d \\ \hline 1 & 1 & a & b & c & d \\ a & a & 1 & c & d & b \\ b & b & d & 1 & a & c \\ c & c & b & d & 1 & a \\ d & d & c & a & b & 1 \end{array} \tag{L5.2}$$

□

Lemma 4. *Let Q be a loop of order 5 in which there exists exactly one $a \in Q$ with $a^2 = 1$, $a \neq 1$. If $L_a \neq R_a$, then the isomorphism type of Q is determined uniquely.*

Proof. By comments above it may be assumed that $R_a \restriction X = \sigma^{-1}$. The rest follows from the unique completion below.

$$\begin{array}{c|ccccc} & 1 & a & b & c & d \\ \hline 1 & 1 & a & b & c & d \\ a & a & 1 & c & d & b \\ b & b & d & & & \\ c & c & b & & & \\ d & d & c & & & \end{array} \quad \to \quad \begin{array}{c|ccccc} & 1 & a & b & c & d \\ \hline 1 & 1 & a & b & c & d \\ a & a & 1 & c & d & b \\ b & b & d & a & 1 & c \\ c & c & b & d & a & 1 \\ d & d & c & 1 & b & a \end{array} \tag{L5.3}$$

□

Lemma 5. *Let Q be a loop of order 5 in which there exists exactly one $a \in Q$ with $a^2 = 1$, $a \neq 1$. There are two classes of isomorphism to which Q may belong if $L_a = R_a$ is assumed. Loops belonging to one of these two classes are opposite (i.e., mirror images) to loops from the other class.*

Proof. Let X and σ be as above. Since $c = 1c = ab = ba = c1$, there must be $c = d^2$. Similarly $b^2 = d$ and $c^2 = b$. The multiplication table is thus known up to products xy, where $x, y \in X$ and $x \neq y$. In each such case $xy \in \{1, a\}$. There two ways how to complete the table:

	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	c	d	1	a
c	c	d	a	b	1
d	d	b	1	a	c

and

	1	a	b	c	d
1	1	a	b	c	d
a	a	1	c	d	b
b	b	c	d	a	1
c	c	d	1	b	a
d	d	b	a	1	c

(L5.4/5)

To see that the two loops are not isomorphic consider the permutation type of L_x, $x \in X$. In the loop upon the left (L5.4) the translations take the form of a 5-cycle. Those upon the right (L5.5) consist of a 3-cycle and a transpozition. □

We have proved that there are **6 isomorphism types of loops of order 5**. One of them is the abelian group, the other are exemplified by tables (L5.1)–(L5.5).

Exercise. Prove that all nonassociative loops of order 5 are isotopic.

Parastrophes and paratopy. A *parastrophe* of a quasigroup $(Q, \cdot)$ is a quasigroup that is equal or opposite to one of the quasigroups $(Q, \cdot)$, $(Q, \backslash)$ and $(Q, /)$. The operation $x * y$ of a parastrophe thus is one of

$$xy,\ x\backslash y,\ x/y,\ yx,\ y\backslash x \text{ and } y/x.$$

It is easy to see that *a parastrophe of a parastrophe of Q is a parastrophe of Q*.

Quasigroups Q_1 and Q_2 are said to be *paratopic* if one of them is isotopic to a parastrophe of the other. The relation 'being paratopic' is (as can be seen easily) an equivalence.

Main class. Two latin squares are *paratopic* if they are multiplication tables of paratopic quasigroups. A *main class* is a class of all latin squares that consists of all latin squares paratopic to one of them. The number of main classes of order n hence coincides with the number of quasigroups of order n up to paratopy. This number is as follows:

n	1	2	3	4	5	6	7	8	9
main classes	1	1	1	2	2	12	147	283 657	19 270 853 541

$n = 10$: 34 817 397 894 749 939

$n = 11$: 2 036 029 552 582 883 134 196 099

The known numbers for isotopy classes are as follows:

n	1	2	3	4	5	6	7	8	9
isotopy cl.	1	1	1	2	2	22	564	1 676 267	115 618 721 533

$n = 10$: 208 904 371 354 363 006

$n = 11$: 12 216 177 315 369 229 261 482 540

Note that for $n \geq 8$ the number of isotopy classes is just a little less than 6 times the number of main classes. This is because with n big enough it becomes less and less likely that a quasigroup is isotopic to one of its nontrivial parastrophes.

The numbers for isomorphism classes of loops:

n	1	2	3	4	5	6	7	8
isomorphism cl.	1	1	1	2	6	109	23 746	106 228 849

$n = 9$: 9 365 022 303 540

$n = 10$: 20 890 436 195 945 769 617

Semisymmetry. What if some parastrophes coincide? If $xy = yx$, then the quasigroup is *commutative*. Multiplication tables of commutative binary operations are symmetric across the main diagonal. If $(Q, \cdot)$ is commutative, then $x\backslash y = y/x$.

What if $xy = y/x$? Let us first show that in each quasigroup every of the following identities implies the other three:

$$x\backslash y = yx \;\Leftrightarrow\; x \cdot yx = y \;\Leftrightarrow\; xy \cdot x = y \;\Leftrightarrow\; xy = y/x. \tag{SS}$$

Proof. It suffices to verify the implication $x \cdot yx = y \;\Rightarrow\; xy \cdot x = y$ since the converse direction follows by a mirror argument. Suppose that $x \cdot yx = y$ holds for all $x, y \in Q$. Then $xy \cdot x = xy \cdot ((x/xy)(xy)) = x/xy$. That is equal to y since $x = y \cdot xy$ is assumed. □

A quasigroup fulfilling the identities of (SS) is called *semisymmetric*. A binary operation is called *semisymmetric* if $x \cdot yx = y = xy \cdot x$. Note that a semisymmetric operation is always a quasigroup operation.

Notational remark. Let $a_1, \ldots, a_k$ be elements of set, say Ω. Then $(a_1\, a_2\, \ldots\, a_k)$ denotes a *cycle* consisting of elements $a_1, \ldots, a_k$. These elements are implicitly assumed to be pairwise distinct. The integer k is the *length* of the cycle. A cycle of length k is called a *k-cycle*. Note that if $k \geq 3$, then

$$(a_1\, a_2\, \ldots\, a_k) = (a_2\, a_3\, \ldots\, a_1) = (a_k\, a_1\, \ldots\, a_{k-1}).$$

Mendelsohn triple systems. Let $\cdot$ be a binary operation on a set Q. Each ordered pair (x, y) initializes a *walk* $a_0, a_1, a_2, \ldots$ upon Q such that $a_0 = x$, $a_1 = y$ and $a_{i+2} = a_i \cdot a_{i+1}$. If the operation is semisymmetric and $x \neq y$, then these walks form cycles $(x\, y\, xy)$ since $y \cdot xy = x$ and $xy \cdot x = y$. If $x = y$, then the cycle shrinks to (x) if $x = xx$, and to $(x\, xx)$ if $x \neq xx$. Recall that a quasigroup Q is called idempotent if $x = xx$.

We have observed that if $\cdot$ is a semisymmetric idempotent operation upon Q, then each ordered pair (x, y), $x \neq y$, occurs in exactly one of the 3-cycles induced by walks of the binary operation. In other words, the 3-cycles of the operation partition the complete oriented graph of Q.

The construction may be reversed. That is, a partition of the complete oriented graph to 3-cycles gives rise to a binary idempotent operation by setting $xy = z$ whenever the partition contains a cycle $(x\, y\, z)$. It is clear that the operation is semisymmetric.

A *Mendelsohn triple system* (MTS) upon Q is a collection of 3-cycles that partitions the complete oriented graph upon Q. Idempotent semisymmetric quasigroups are also known as *MTS quasigroups*.

An example of an MTS on a 4-element set: cycles $(a\, b\, c)$, $(c\, b\, d)$, $(b\, a\, d)$ and $(a\, c\, d)$. The multiplication table:

	a	b	c	d
a	a	c	d	b
b	d	b	a	c
c	b	d	c	a
d	c	a	b	d

Challenge. Occurences of each symbol in the body of the multiplication table above may be connected by moves of a chess knight. Construct further examples of such latin squares. Are there other examples that may be obtained from an MTS quasigroup?

Steiner triple systems. A semisymmetric operation that is commutative yields a quasigroup in which all parastrophes coincide. This is why such quasigroups are called *totally symmetric.*

What are the commutative MTS quasigroups, i.e., idempotent totally symmetric quasigroups? The commutativity implies that with each cycle $(a\,b\,c)$ there is a cycle $(c\,b\,a)$. The cycles may be thus replaced by 3-element sets. What arises is a collection of 3-element subsets (called *blocks*) such that each 2-element subset is contained in exactly one block. These are the *Steiner triple systems* (STS).

An STS of order n exists for each $n \equiv 1, 3 \bmod 6$. Numbers of STS up to isomorphism is given by the following table.

n	1	3	7	9	13	15	19
STS up to $\cong$	1	1	1	1	2	80	11 084 874 829

Prolongation. Let $(Q,*)$ be an idempotent quasigroup. Assume that Q does not contain the symbol 1. Define an operation $\cdot$ upon $\hat{Q} = Q \cup \{1\}$ in such a way that

$$x \cdot 1 = 1 \cdot x = x,\ 1 \cdot 1 = 1 = x \cdot x \text{ and } x \cdot y = x * y$$

whenever $x, y \in Q$ and $x \neq y$. Then $\hat{Q}$ is a loop. The construction may be reversed whenever starting from a loop Q such that $x^2 = 1$ for each $x \in Q$.

Proposition. *A prolongation of an idempotent totally symmetric quasigroup is totally symmetric, and all totally symmetric loops may be obtained in this way.*

Proof. Let $(Q,*)$ be idempotent. It is clear that $\hat{Q}$ is commutative if and only if $(Q,*)$ is commutative. Hence it is enough to show (1) that $\hat{Q}$ is semisymmetric if and only if $(Q,*)$ is semisymmetric, and (2) that each semisymmetric loop fulfils $x^2 = 1$. The latter is clear since $1 = (x \cdot 1)x = x^2$, by semisymmetry. For the former property note that $(x*y)*x = y$ if $x = y$. If $x \neq y$, then $x*y \neq x*x = x$, and thus $(x*y)*x = xy \cdot x$. On the other hand in $\hat{Q}$ the identity $xy \cdot x = y$ holds whenever $x = y$ or $1 \in \{x, y\}$. If $x \neq y$ and $1 \notin \{x, y\}$, then $xy \neq x$ and $xy \cdot x = (x*y)*x$. □

Note that by the proof *prolongations of MTS quasigroups are exactly the semisymmetric loops.*

Affine and projective STS. Let V be a vector space over a 3-element field. The affine lines of V form an STS. Such STS are called *affine.* The idempotent operation of the STS over V may be expressed by $x * y = -x - y$.

A *Hall Triple System* (HTS) is an STS such that any two intersecting blocks belong to a subsystem on 9 elements. (There is only one STS of order 9, and this STS coincides with the affine plane of order 3.) Structure of Hall Triple Systems will be investigated later in this course.

Consider a projective space over a 2-element field. If the space is of dimension n, then it contains $2^{n+1} - 1$ points. Each line consists of three elements and any three noncollinear points belong to a Fano subplane. The lines form an STS. Such an STS is called *projective.*

Let $(Q,*)$ be the idempotent quasigroup of a projective STS. Suppose that x, y, z do not belong to the same block (they are noncollinear). Consider the picture of the Fano plane with x, y and z being the three vertices of the triangle that forms the picture. Then $(x*y)*z = x*(y*z)$ is the central element. This implies that the prolongation yields an associative loop $\hat{Q}$. In this loop (which is a group) $x^2 = 1$ for each $x \in Q$. This means that $\hat{Q}$ has to be an elementary abelian 2-group.

All projective STS thus may be derived from nonzero elements of an elementary abelian 2-group. Blocks coincide with subgroups of order 4 from which the zero is removed.