Simula UiB Summer internship results

Håvard Skjetne Lilleheie

25/07/2023

1 Universal definitons

Definition 1.1. Let $[n] = \{0, 1, \ldots, n-1\}$.

Definition 1.2. Let $\mathrm{Sym}(n) = \{\text{Permutations from } [n] \text{ to } [n]\}$.

2 Abelian group results

Definition 2.1. Let $n \in \mathbb{N}$, then $\mathrm{Ab}(n) = \{\text{All Abelian Groups over the elements } [n]\}$.

Theorem 2.2. *Let $H \in \mathrm{Ab}(n)$, and let $\phi \in \mathrm{Sym}(n)$.*

Let $S = ([n], +_S)$ be a set over $[n]$ with a binary operation $+_S$ defined by

$$a +_S b = \phi(\phi^{-1}(a) +_H \phi^{-1}(b)) \tag{1}$$

Then $S \in \mathrm{Ab}(n)$.

Proof. TODO2 $\qquad\square$

Remark 2.3. The equation in Equation 1 is equivalent to:

$$a +_H b = \phi^{-1}(\phi(a) +_S \phi(b)).$$

Definition 2.4. Let $H \in \mathrm{Ab}(n)$, and let $\phi \in \mathrm{Sym}(n)$.

Then the *conjugacy of H with respect to ϕ* is the abelian group S as defined in Theorem 2.2. And it is denoted by $\phi(H)$.

Theorem 2.5. *Let $H \in \mathrm{Ab}(n)$ and let $\phi \in \mathrm{Sym}(n)$.*

Then ϕ is an isomorphism from H to $\phi(H)$.

Proof. Look at

$$\phi(a +_H b) = \phi(\phi^{-1}(\phi(a) +_{\phi(H)} \phi(b))) = \phi(a) +_{\phi(H)} \phi(b)$$

Which is the definition of a homomorphism. And since ϕ is a bijection, it is thereofre an isomorphism. $\qquad\square$

Remark 2.6. For $H \in Ab(n)$, then the set of conjugacies of H, i.e.

$$\{\phi(H) : \phi \in \text{Sym}(n)\}$$

is exactly the isomorphism class of H.

Theorem 2.7. *Let $\phi : H \to S$ be an isomorphism.*

Then $\lambda \in \text{Aut}(H) \iff \phi \circ \lambda \circ \phi^{-1} \in \text{Aut}(S)$.

Proof. Show first $\Rightarrow$:

Let $\lambda \in Aut(H)$. Then

$$
\begin{aligned}
\phi \circ \lambda \circ \phi^{-1}(a +_S b) &= \phi \circ \lambda(\phi^{-1}(a) +_H \phi^{-1}(b)) \\
&= \phi(\lambda \circ \phi^{-1}(a) +_H \lambda \circ \phi^{-1}(b)) \\
&= \phi \circ \lambda \circ \phi^{-1}(a) +_S \phi \circ \lambda \circ \phi^{-1}(b)
\end{aligned}
$$

Which is the definition of $\phi \circ \lambda \circ \phi^{-1} \in \text{Aut}(S)$

Show then $\Leftarrow$:

Let $\phi \circ \lambda \circ \phi^{-1} \in \text{Aut}(S)$, and let $\tilde{a} = \phi(a)$. Then

$$\phi \circ \lambda \circ \phi^{-1}(\tilde{a} +_S \tilde{b}) = \phi \circ \lambda \circ \phi^{-1}(\tilde{a}) +_S \phi \circ \lambda \circ \phi^{-1}(\tilde{b})$$

$$\Updownarrow$$

$$\phi^{-1} \circ \phi \circ \lambda \circ \phi^{-1}(\tilde{a} +_S \tilde{b}) = \phi^{-1}(\phi \circ \lambda \circ \phi^{-1}(\tilde{a}) +_S \phi \circ \lambda \circ \phi^{-1}(\tilde{b}))$$

$$\lambda \circ \phi^{-1}(\tilde{a} +_S \tilde{b}) = \phi^{-1} \circ \phi \circ \lambda \circ \phi^{-1}(\tilde{a}) +_H \phi^{-1} \circ \phi \circ \lambda \circ \phi^{-1}(\tilde{b})$$

$$\lambda(\phi^{-1}(\tilde{a}) +_H \phi^{-1}(\tilde{b})) = \lambda \circ \phi^{-1}(\tilde{a}) +_H \lambda \circ \phi^{-1}(\tilde{b})$$

$$\lambda(\phi^{-1}(\phi(a)) +_H \phi^{-1}(\phi(b))) = \lambda \circ \phi^{-1}(\phi(a)) +_H \lambda \circ \phi^{-1}(\phi(b))$$

$$\lambda(a +_H b) = \lambda(a) +_H \lambda(b) \qquad \square$$

Remark 2.8. From Theorem 2.5 and Theorem 2.7 one has that taking any Abelian group G over $[n]$ with identity element $e \in [n]$, and setting $\phi = (0, e)$, one gets that any automorphism over G can be "transformed" to an automorphism over $(i, 0)(G)$ where 0 is the identity, and vice versa. Therefore one only need to look at the automorphisms of abelian groups where 0 is a fixed identity to look for classifications of permutation as automorphisms.

Theorem 2.9. *Let S be a set with a closed binary operation $*_S$ that is*

- *associative, and*

- *commutative, and*

- *where for any $a \in S$, the map $x \mapsto x *_S a$ is a bijection,*

has an identity element. And is therefore an Abelian group.

Proof. Let a be any element in the group. Since $a + x$ is a bijection, there exist a y such that $a + y = a$. Want to prove that this y is in fact an identity element for the binary operation.

Assume $b + y = z$ for some z. adding a to both sides gives an equivalent equation: $a + (b + y) = a + z$. Using associativity, this becomes: $(a + b) + y = a + z$. Then from commutativity one

gets $(b + a) + y = a + z$. Using associativity again, one gets: $b + (a + x) = a + z$. But since $a + y = a$ by assumption, this reduces to: $b + a = a + z$. But since the operation $a + x$ is a bijection, it is then injective, and hence $z = b$, which implies $b + y = b$. Since the choice of b was arbitrary, y is the identity element. $\square$

Remark 2.10. For every $\phi \in \text{Sym}(n)$, and for every $H \in \text{Ab}(n)$, if $a = b +_H b$, then $\phi(a) = \phi(b) +_{\phi(H)} \phi(b)$. This implies that any element on the diagonal of the group operation table stays on the diagonal of the group operation table, but permuted.

For example, consider the case when $\phi(0) = 0$, then one has that the conjugate must have the exact same amount of zeros on the diagonal.

Definition 2.11. Let $\text{Ab}_0(n)$ denote the subset of $\text{Ab}(n)$ where 0 is the identity of the abelian groups.

Theorem 2.12. $\dfrac{\# \text{Ab}(n)}{\# \text{Ab}_0(n)} = n$

Proof. In order to prove this, we need to add a temporary definition:

Let $\text{Ab}_i(n)$ denote the subset of $\text{Ab}(n)$ where $i \in [n]$ is the identity element.

Then we have to prove three different lemmas:

First lemma: $\text{Ab}_i(n) \cap \text{Ab}_j(n) = \emptyset$ for $i \neq j$.

Proof of first lemma: Assume $\text{Ab}_i(n) \cap \text{Ab}_j(n) \neq \emptyset$. Then there exists an abelian group $G \in \text{Ab}_i(n) \cap \text{Ab}_j(n)$ that has both i and j as an identity element. But then $i = i *_G j = j$, which is a contradiction, and $\text{Ab}_i(n) \cap \text{Ab}_j(n) = \emptyset$, since the identity must be unique.

Second lemma: $\text{Ab}(n) = \cup_{i=0}^{n-1} \text{Ab}_i(n)$

Proof of second lemma: First show $\subseteq$: Let $G \in \text{Ab}(n)$. Then, by definition, G has an identity element, let's say $e \in [n]$. But then $G \in \text{Ab}_e(n)$. Therefore $\text{Ab}(n) \subseteq \cup_{i=0}^{n-1} \text{Ab}_i(n)$.

Then show $\supseteq$: Every $\text{Ab}_j(n) \subseteq \text{Ab}(n)$ by definition. Therefore it follows that $\text{Ab}(n) \supseteq \cup_{i=0}^{n-1} \text{Ab}_i(n)$.

Third lemma: $\# \text{Ab}_i(n) = \# \text{Ab}_j(n)$ for all $i, j \in [n]$.

Proof of third lemma: Let $\phi = (i, j)$. Then one can define a map:

$$\varphi : \text{Ab}_i(n) \to \text{Ab}_j(n)$$
$$G \mapsto \phi(G)$$

Want to show that this map is a bijection, and therefore preserves the cardinality of the sets.

First, let's show that φ is injective: Let $G, H \in \text{Ab}_i(n)$ and let $\tilde{a} = \phi(a)$ and $\tilde{b} = \phi(b)$.

Then

$$\varphi(G) = \varphi(H)$$
$$\phi(G) = \phi(H)$$
$$\Downarrow$$
$$\tilde{a} +_{\phi(G)} \tilde{b} = \tilde{a} +_{\phi(H)} \tilde{b}$$
$$\phi(\phi^{-1}(\tilde{a}) +_G \phi^{-1}(\tilde{b})) = \phi(\phi^{-1}(\tilde{a}) +_H \phi^{-1}(\tilde{b}))$$
$$\Updownarrow$$
$$\phi^{-1}(\phi(\phi^{-1}(\tilde{a}) +_G \phi^{-1}(\tilde{b}))) = \phi^{-1}(\phi(\phi^{-1}(\tilde{a}) +_H \phi^{-1}(\tilde{b})))$$
$$\phi^{-1}(\tilde{a}) +_G \phi^{-1}(\tilde{b}) = \phi^{-1}(\tilde{a}) +_H \phi^{-1}(\tilde{b})$$
$$a +_G b = a +_H b$$

So G and H are groups with the same group operation over the exact same set. They are therefore equal, i.e. $G = H$.

Secondly, lets show that φ is surjective: Let $K \in \mathrm{Ab}_j(n)$. Then want to show that $\varphi(\phi^{-1}(K)) = \phi(\phi^{-1}(K)) = K$.

First, note that $a +_{\phi^{-1}(K)} b = \phi^{-1}(\phi(a) +_K \phi(b))$. Then

$$\begin{aligned}
a +_{\phi(\phi^{-1}(K))} b &= \phi(\phi^{-1}(a) +_{\phi^{-1}(K)} \phi^{-1}(b)) \\
&= \phi(\phi^{-1}(\phi(\phi^{-1}(a)) +_K \phi(\phi^{-1}(b))))) \\
&= \phi(\phi^{-1}(a)) +_K \phi(\phi^{-1}(b)) \\
&= a +_K b
\end{aligned}$$

So K and $\phi(\phi^{-1}(K))$ are groups with the same group operation over the exact same set. They are therefore equal, i.e. $K = \phi(\phi^{-1}(K))$.

So for the proof of the theorem: The first and the second lemma gives that $\mathrm{Ab}(n)$ is a disjoint union of $\{\mathrm{Ab}_i(n) : i \in [n]\}$. Therefore $\# \mathrm{Ab}(n) = \sum_{i=0}^{n-1} \# \mathrm{Ab}_i(n)$. But the third lemma says that $\mathrm{Ab}_i(n) = \mathrm{Ab}_0(n)$ for all i. Therefore $\# \mathrm{Ab}(n) = \sum_{i=0}^{n-1} \# \mathrm{Ab}_0(n) = n \# \mathrm{Ab}_0(n)$ which implies $\frac{\# \mathrm{Ab}(n)}{\# \mathrm{Ab}_0(n)} = n$. $\qquad\square$

Theorem 2.13. *Let $H \in \mathrm{Ab}(n)$.*

Then for every $a \in H$, the map $\varphi_a : x \mapsto x +_H a$ is a bijection.

Proof. Assume there exists an $a \in H$ such that φ_a is not a bijection.

Since $\varphi_a : H \to H$, and H has finite cardinality. Then φ_a is not injective. This implies that there exist to values $x \neq y$ such that $x +_H a = y +_H a$. But using the latter equation and adding $-a$ to both sides, one gets that $x = y$ which is a contradiction. $\qquad\square$

Remark 2.14. The property in Theorem 2.13 is the *latin square property*, which will be further studied later.

Counterexample 2.15. Let $\phi \in \mathrm{Sym}(n)$ with $\phi(0) = 0$.

Then there *does not necessarily* exist a $H \in \mathrm{Ab}_0(n)$ such that $\phi \in \mathrm{Aut}(H)$.

Special case. Let $\phi = (3, 4)$, there want to show that there are no groups H in $\text{Ab}_0(5)$ where $\phi \in \text{Aut}(H)$ with a proof by contradiction.

Assume ϕ is an automorphism for $H \in G_0(5)$.

Then $\phi(1 +_H 1) = \phi(1) +_H \phi(1) = 1 +_H 1$, and $\phi(2 +_H 2) = \phi(2) +_H \phi(2)$, and $\phi(1 +_H 2) = \phi(1) +_H \phi(2) = 1 +_H 2$. This means that $1 +_H 1, 2 +_H 2, 1 +_H 2 \in \{0, 1, 2\}$, since they are fixed points of the map ϕ. And the set $\{0, 1, 2\}$ is therefore closed under the group operation.

Furthermore, since $1 +_H 2$ can not be 1 or 2, since that would imply that either 1 or 2 is an identity, then $1 +_H 2 = 0$, and the set $\{0, 1, 2\}$ is therefore a subgroup of H, since every element in $\{0, 1, 2\}$ has an inverse. But H has order 5, which 3 does not divide which contradicts Lagrange's theorem, and therefore ϕ can not be an automorphism. $\qquad\square$

General case. Let $n \geq 5$, and let $\phi \in \text{Sym}(n)$ with $\phi = (n - 2, n - 1)$. Want to do a proof by contradiction to show that there are no groups $H \in \text{Ab}_0(n)$ such that $\phi \in \text{Aut}(H)$.

Assume $\phi \in \text{Aut}(H)$.

Then for $i, j \in [n - 3]$ one has that $\phi(i +_H j) = \phi(i) +_H \phi(j) = i +_H j$. So $i +_H j \in [n - 3]$ since it is a fixed point of ϕ. But then one has that the top left $(n - 2) \times (n - 2)$ square of the group operation table of H only contains elements in $[n - 3]$. One has by the latin square property (Theorem 2.13) that the remaining two elements, $n - 2$ and $n - 1$ has to appear once for every row of the top right rectangle with the shape $(n - 2) \times (2)$, since the elements doesn't appear in any of the rows in the top left $(n - 2) \times (n - 2)$ square of the group operation table. However, since $n \geq 5$, the top right rectangle has a height of at least 3, which is greater than it's width. One would therefore have one column where the same element would appear at least twice, which also breaks the latin square property. Therefore $\phi \notin \text{Aut}(H)$. $\qquad\square$

Counterexample 2.16. Let $\phi \in \text{Sym}(n)$.

Then there *does not neccesarily* exist a $H \in Ab(n)$ with $a \in H$ such that the map $x \mapsto x +_H a$ is equal to ϕ.

Proof. This is the exact same result as Counterexample 2.18. $\qquad\square$

Definition 2.17. For $H \in \text{Ab}(n)$,

then let $\text{AAut}(H) := \{\phi(\_) +_H v : \phi \in \text{Aut}(H) \wedge v \in H\}$.

Counterexample 2.18. Let $\phi \in \text{Sym}(n)$.

Then there *does not necessarily* exist an $H \in \text{Ab}(n)$ such that $\phi \in \text{AAut}(H)$.

Proof. Let $\phi = (3, 4)$. Want to show that ϕ is not an affine automorphism for any group H in $\text{Ab}(5)$.

We will do a proof by contradiction by assuming that $\phi \in \text{AAut}(H)$, and getting a contradiction. We have to look at two different cases to prove this. First when the identity is $0, 1,$ or 2. And then secondly when the identity is either 3 or 4.

Assume that $\phi \in \text{AAut}(H)$. Denote the identity of H by "e". Furthermore let $\alpha \in \text{Aut}(H)$ and $\tilde{v} \in H$ be the elements such that $\phi(\_) = \alpha(\_) +_H \tilde{v}$.

Let $v = -\tilde{v}$.

This gives that $\alpha(\_) = \phi(\_) +_H (-\tilde{v}) = \phi(\_) +_H v$.

Then one has that
$$e = \alpha(e) = \phi(e) +_H v.$$

This gives us that $v = -\phi(e)$.

Case 1: Assume that $e \in \{0, 1, 2\}$.

Then one has that $v = -e = e$. So then $\phi \in \text{Aut}(H)$ by the assumption.

This gives us that $\{0, 1, 2\}$ is a subgroup of H, since for $a, b \in \{0, 1, 2\}$ then $\phi(a +_H b) = \phi(a) +_H \phi(b) = a +_H b$, which makes $a +_H b$ a fixed-point of ϕ, and therefore $a +_H b \in \{0, 1, 2\}$. Furthermore $0 +_H 1 +_H 2 = e$ since $e \in \{0, 1, 2\}$, so the identity element can be removed from the sum, and the elements left have to sum to the identity or else there would be two different identities, which is not possible in a group. Therefore every element has it's inverse in $\{0, 1, 2\}$. Along with associativity from H, then the set $\{0, 1, 2\}$ is a subgroup of order 3.

This is *not possible* since every subgroup of H, which has order 5, must divide it's order by Lagrange's theorem.

Case 2: Assume that $e \in \{3, 4\}$. Without loss of generality assume $e = 3$.

Then one has that $v = -\phi(3) = -4$. And specifically one has that

$$\alpha(4) = \phi(4) - 4 = 3 -_H 4 = -4$$

And by the homomorphism property, $\alpha(-4) = -\alpha(4) = -(-4) = 4$

In general notice that

$$\alpha(i) = \begin{cases} i -_H 4 & i \in \{0, 1, 2\} \\ 3 & i == 3 \\ -4 & i == 4 \end{cases}$$

This gives the identity: $\alpha(\alpha(i)) = i$. So α is it's own inverse, and therefore it must be a composition of zero, one or two disjoint transmutations.

We further split this up into two cases:

Case 2.1: Assume α has a fixed-point besides 3.

Then by the fact that α is the composition of zero, one or two disjoint transmutations, it must be either identity or one transmutation. This implies there is at least one fixed-point among $\{0, 1, 2\}$. Without loss of generality, assume this fixed element is 0. Then $0 = \alpha(0) = 0 -_H 4$. But subtracting 0 on either side, on gets that $3 = -4$, which is not true, since then $3 = 4 -_H 4 = 4 +_H 3 = 4$, which is not true.

Case 2.2: Assume α has no fixed-points beside 3. Without loss of generality, assume $\alpha = (0, 4)(1, 2)$

Then

$$1 +_H 2 = 1 -_H 4 +_H 2 -_H 4 +_H 4 +_H 4 = \alpha(1) + \alpha(2) +_H 4 +_H 4 = 2 +_H 1 +_H 4 +_H 4.$$

But by adding $-(1 +_H 2)$ to both sides, one gets: $4 +_H 4 = 3$. However, this implies $4 = -4 = \alpha(4) = 0$, which is not true. $\qquad \square$

3 LatinSquare/Quasigroup

Definition 3.1. Let Q be a set with a binary operation $\_ *_Q \_$ with the following properties:

1. $\_ *_Q \_$ is closed.

2. For every $a \in Q$, the map $x \mapsto a *_Q x$ is a bijection.

3. For every $a \in Q$, the map $x \mapsto x *_Q a$ is a bijection.

Remark 3.2. Item number 2 and 3 in the requirements of a quasigroup are called the "latin square property" because these rules are equivalent to that the group operation table is a latin square.

Definition 3.3. Let $\mathrm{Quas}(n)$ denote the set of all quasigroups over $[n]$.

Theorem 3.4. *An associative quasigroup is a group.*

For a proof, see [anassociativequasigroupisagroup](#).

Counterexample 3.5. A commutative quasigroup is not an abelian group.

Proof. TODO ☐

Definition 3.6. A loop is a quasigroup with a (unique) two-sided identity element.

Counterexample 3.7. A commutative loop is not an abelian group.

Proof. TODO ☐

Theorem 3.8. *Any quasigroup in* $\mathrm{Quas}(n)$ *can be represented as an* $n \times n$ *latin square by their group operation table.*

Proof. From [Remark 3.2](#), one has that the group operation table of a quasigroup is a latin square.

Given an $n \times n$ latin square, look at the binary operation induced by the latin square. It satisfies all the quasigroup properties, and therefore the set $[n]$ with this binary operation is a quasigroup. ☐

Theorem 3.9. *Let* $H \in \mathrm{Quas}(n)$ *and let* $\phi \in \mathrm{Sym}(n)$.

Then let $S = ([n], *_S)$ *be a set with a binary operation where* $*_S$ *is given by:*

$$a *_S b = \phi(\phi^{-1}(a) *_H \phi^{-1}(b)).$$

Then S *is a quasigroup.*

Definition 3.10. Let $\phi \in \mathrm{Sym}(n)$, and let $Q \in \mathrm{Quas}(n)$.

Then the *conjugacy of Q with respect to* is the quasigroup S from [Theorem 3.9](#). This S is denoted as $\phi(Q)$.

Remark 3.11. The definition in [Definition 3.10](#) reflects the definition for abelian groups in [Definition 2.4](#), but for quasigroups.

Theorem 3.12. *Let* $\phi \in \mathrm{Sym}(n)$, *and let* $Q \in \mathrm{Quas}(n)$.

Then $\phi \in \mathrm{Aut}(H) \iff \phi(Q) = Q$.

Proof. TODO □

Lemma 3.13. *Let $\alpha, \beta, \gamma \in Sym(n)$, and let Q be any quasigroup over $[n]$.*

Then there exist a unique quasigroup, denoted $(\alpha, \beta, \gamma)(Q)$, such that (α, β, γ) is an isotopy from Q to $(\alpha, \beta, \gamma)(Q)$.

Proof. TODO □

Remark 3.14. TODO: Similar to definition of conjugacy.

Definition 3.15. Let $\phi \in Sym(n)$.

If there exist a $\lambda \in Aut(Q)$ and $v \in Q$, such that at least one of the following is true:

- $\phi(\_) = \lambda(\_)$, or

- $\phi(\_) = \lambda(\_) *_Q v$, or

- $\phi(\_) = v *_Q \lambda(\_)$.

Then $\phi \in AAut(Q)$.

Remark 3.16. TODO: Very similar to Ab definiton.

Construction 3.17. *For $\phi \in Sym(n)$.*

Then for any given quasigroup Q with left (right) identity. One can construct another quasigroup $\tilde{Q}$ such that $\phi \in AAut(\tilde{Q})$.

Proof. TODO: Let L be any loop (Probably a quasigroup with left-identity would be sufficient) over $[n]$, with identity element e.

Let Q be the quasigroup over $[n]$ such that (Id, φ^{-1}, Id) is an isotopy from L to Q as mentioned in Lemma 3.13.

Then from the isometry property $Id(x) *_Q \varphi^{-1}(y) = Id(x *_L y)$, one gets:

$$x *_L \varphi(y) = Id(x *_L \varphi(y)) = Id(x) *_Q \varphi^{-1}(\varphi(y)) = x *_Q y$$

Using $x *_Q y = x *_L \varphi(y)$ and taking $x = e$, one gets: $e *_Q y = e *_L \varphi(y) = \varphi(y)$. But then $\varphi(y) = e *_Q id(y)$, and hence $\varphi(y) \in AAut(Q)$, since $id \in Aut(Q)$ and $e \in Q$. □

Remark 3.18. TODO: In fact, the quasigroup created in the proof for **??** has a right-identity, namely $\varphi^{-1}(e)$, since for any $x \in Q$, one has $x *_Q \varphi^{-1}(e) = x *_L e = x$.

Lemma 3.19. *TODO: Let $\varphi \in Sym(n)$, and let Q be a commutative quasigroup over $[n]$.*

*Then the quasigroup, $\tilde{Q}$, over $[n]$ such that (φ, φ, Id) is an isotopy from from Q to $\tilde{Q}$ as mentioned in **??**, is also commutative.*

Proof. TODO: From the isotopy property $x *_Q y = \varphi^{-1}(x) *_{\tilde{Q}} \varphi^{-1}(y)$. Therefore one gets $x *_{\tilde{Q}} y = \varphi(x) *_Q \varphi(y) = \varphi(y) *_Q \varphi(x) = y *_{\tilde{Q}} x$. □

Corollary 3.20. *TODO: Let $\varphi \in Sym(n)$.*

Then there exist a commutative quasigroup, Q, such that $\varphi \in AAut(Q)$.

Proof. TODO: Let A be any abelian group (commutative loop would probably had been sufficient) over $[n]$, with identity element e.

Let Q be the commutative quasigroup over $[n]$ such that $(\varphi^{-1}, \varphi^{-1}, Id)$ is an isotopy from A to Q as mentioned in Lemma 3.19.

Then from the isometry property $\varphi^{-1}(x) *_Q \varphi^{-1}(y) = Id(x *_A y)$, one gets:

$$\varphi(x) *_A \varphi(y) = Id(\varphi(x) *_A \varphi(y)) = \varphi^{-1}(\varphi(x)) *_Q \varphi^{-1}(\varphi(y)) = x *_Q y$$

Using $x *_Q y = \varphi(x) *_A \varphi(y)$ and taking $x = \varphi^{-1}(e)$, one gets: $\varphi^{-1}(e) *_Q y = e *_A \varphi(y) = \varphi(y)$. But then $\varphi(y) = \varphi^{-1}(e) *_Q id(y)$, and hence $\varphi(y) \in AAut(Q)$, since $id \in Aut(Q)$ and $\varphi^{-1}(e) \in Q$. $\qquad\square$

Theorem 3.21. *TODO: Let Q be a quasigroup over $[n]$ with left (right) identity, and let $\varphi(\pi) \in Sym(n) \setminus \{id\}$ have a fixed point.*

*Then for any $\pi(\varphi) \in Sym(n)$, every isotopy image (**??**) of (π, φ, id) of Q does not have a left (right) identity. In particular, it is not a loop.*

Proof. TODO: Let H denote the isotopy image.

The isotopy property says that $\pi(x) *_H \varphi(y) = x *_Q y$, or equivalently, $x *_H y = \pi^{-1}(x) *_Q \varphi^{-1}(y)$.

Let a be a fixed point of φ from the assumption, and let b be a non-fixed point of φ (we know it must exist since by assumption $\varphi \neq id$). Furthermore, let e denote the right-identity of Q.

Then $\pi(e) *_H a = e *_Q \varphi^{-1}(a) = e *_Q a = a$, and from the quasigroup/latin square property, one has that $\pi(e)$ has to be the unique left identity if it exists. However, $\pi(e) *_H b = e *_Q \varphi^{-1}(b) = \varphi^{-1}(b) \neq b$, so $\pi(e)$ cannot be a left identity, and H therefore has no left identity. $\qquad\square$

Remark 3.22. TODO: The above theorem would imply that in general, for any permutation it might not be possible to find a loop where it is an affine automorphism using our previous construction. And since an associative quasigroup is a group, and therefore a loop, it might not be possible to get an operation that is associative.