Linear aspects of quasigroup triality

Alex W. Nowak
Iowa State University

Dissertation Defense

April 13, 2020

Summary

Quasigroups and triality

Triality: a combinatorial perspective

- $(Q, \cdot)$ is a quasigroup when $T = \{(x, y, x \cdot y) \mid (x, y) \in Q^2\}$ has the *Latin square property*:
  - $\forall (x_1, x_2, x_3), (y_1, y_2, y_3) \in T,\ |\{1 \leq i \leq 3 \mid x_i = y_i\}| \neq 2.$
- For all $g \in S_3$, $T^g = \{(x_{1g}, x_{2g}, x_{3g}) \mid (x_1, x_2, x_3) \in T\}$ also has the Latin square property.
- If H is a subgroup of the kernel of this permutation action, then T is H-symmetric.

Triality: a combinatorial perspective

- $(Q, \cdot)$ is a quasigroup when $T = \{(x, y, x \cdot y) \mid (x, y) \in Q^2\}$ has the *Latin square property*:
  - $\forall (x_1, x_2, x_3), (y_1, y_2, y_3) \in T,\ |\{1 \leq i \leq 3 \mid x_i = y_i\}| \neq 2$.
- For all $g \in S_3$, $T^g = \{(x_{1g}, x_{2g}, x_{3g}) \mid (x_1, x_2, x_3) \in T\}$ also has the Latin square property.
- If H is a subgroup of the kernel of this permutation action, then T is H-symmetric.

Triality: a combinatorial perspective

- $(Q, \cdot)$ is a quasigroup when $T = \{(x, y, x \cdot y) \mid (x, y) \in Q^2\}$ has the *Latin square property*:
  - $\forall (x_1, x_2, x_3), (y_1, y_2, y_3) \in T,\ |\{1 \leq i \leq 3 \mid x_i = y_i\}| \neq 2.$
- For all $g \in S_3$, $T^g = \{(x_{1g}, x_{2g}, x_{3g}) \mid (x_1, x_2, x_3) \in T\}$ also has the Latin square property.
- If H is a subgroup of the kernel of this permutation action, then T is H-symmetric.

Triality: an algebraic perspective

- $(Q, \cdot, /, \backslash)$ is a quasigroup when all the following hold:

$$\begin{aligned} &\text{(IL)} \quad y\backslash(y \cdot x) = x, && \text{(IR)} \quad x = (x \cdot y)/y, \\ &\text{(SL)} \quad y \cdot (y\backslash x) = x, && \text{(SR)} \quad x = (x/y) \cdot y. \end{aligned}$$

$$\begin{tikzcd}
 & (Q,\cdot,/,\backslash) \arrow[r, leftrightarrow, "(12)"] \arrow[dl, Leftrightarrow, "(23)"'] & (Q,\circ,\backslash\backslash,//) \arrow[dr, Leftrightarrow, "(23)"] & \\
(Q,\backslash,//,\cdot) \arrow[dr, leftrightarrow, "(12)"'] & & & (Q,\backslash\backslash,\circ,/) \arrow[dl, leftrightarrow, "(12)"] \\
 & (Q,//,\backslash,\circ) \arrow[r, Leftrightarrow, "(23)"'] & (Q,/,\cdot,\backslash\backslash) &
\end{tikzcd}$$

Triality: an algebraic perspective

- $(Q, \cdot, /, \backslash)$ is a quasigroup when all the following hold:

$$
\begin{aligned}
&\text{(IL)}\quad y\backslash(y\cdot x) = x, &\qquad &\text{(IR)}\quad x = (x\cdot y)/y,\\
&\text{(SL)}\quad y\cdot(y\backslash x) = x, &\qquad &\text{(SR)}\quad x = (x/y)\cdot y.
\end{aligned}
$$

$$
\begin{tikzcd}
 & (Q, \cdot, /, \backslash) \arrow[r, leftrightarrow, "(12)"] \arrow[dl, Leftrightarrow, "(23)"'] & (Q, \circ, \backslash\backslash, //) \arrow[dr, Leftrightarrow, "(23)"] & \\
(Q, \backslash, //, \cdot) \arrow[dr, leftrightarrow, "(12)"'] & & & (Q, \backslash\backslash, \circ, /) \arrow[dl, leftrightarrow, "(12)"] \\
 & (Q, //, \backslash, \circ) \arrow[r, Leftrightarrow, "(23)"'] & (Q, /, \cdot, \backslash\backslash) &
\end{tikzcd}
$$

Multiplication groups

- $(Q, \cdot)$ is a quasigroup iff $R(q) : x \mapsto x \cdot q$ and $L(q) : x \mapsto q \cdot x$ are bijections.
- The group $\mathrm{Mlt}(Q) = \langle R(q), L(q) \rangle_{S_Q}$ acts transitively on Q.
- Q is a subquasigroup of $Q[X] = Q \coprod_{\mathbf{V}} \langle X \rangle_{\mathbf{V}}$ and the subgroup of $\mathrm{Mlt}(Q[X])$ generated by $R(Q) \cup L(Q)$ is the *universal multiplication group of Q in $\mathbf{V}$*, $U(Q; \mathbf{V})$.

Multiplication groups

- $(Q, \cdot)$ is a quasigroup iff $R(q) : x \mapsto x \cdot q$ and $L(q) : x \mapsto q \cdot x$ are bijections.
- The group $\mathsf{Mlt}(Q) = \langle R(q), L(q) \rangle_{S_Q}$ acts transitively on Q.
- Q is a subquasigroup of $Q[X] = Q \coprod_{\mathbf{V}} \langle X \rangle_{\mathbf{V}}$ and the subgroup of $\mathsf{Mlt}(Q[X])$ generated by $R(Q) \cup L(Q)$ is the *universal multiplication group of* Q *in* $\mathbf{V}$, $U(Q; \mathbf{V})$.

Multiplication groups

- $(Q,\cdot)$ is a quasigroup iff $R(q): x \mapsto x\cdot q$ and $L(q): x \mapsto q\cdot x$ are bijections.
- The group $\mathsf{Mlt}(Q) = \langle R(q), L(q)\rangle_{S_Q}$ acts transitively on Q.
- Q is a subquasigroup of $Q[X] = Q \coprod_{\mathbf{V}} \langle X\rangle_{\mathbf{V}}$ and the subgroup of $\mathsf{Mlt}(Q[X])$ generated by $R(Q)\cup L(Q)$ is the *universal multiplication group of Q in $\mathbf{V}$*, $U(Q;\mathbf{V})$.

Universal stabilizers

- $U(Q;\mathbf{V})$ also acts transitively on Q, so for any $e \in Q$, define $U(Q;\mathbf{V})_e$ to be the *universal stabilizer of Q in $\mathbf{V}$*.

$$
\begin{tikzcd}
 & rq & \\
e \arrow[ur, bend left, "L(rq/e)"] \arrow[rr, bend left, "L(q/e)"] \arrow[rr, bend right, "R(e\backslash q)"'] \arrow[dr, bend right, "R(e\backslash qr)"'] & & q \arrow[ul, bend right, "L(r)"'] \arrow[dl, bend left, "R(r)"] \\
 & qr &
\end{tikzcd}
$$

- Define $T_e(q) = R(e\backslash q)L(q/e)^{-1}$, $R_e(q,r) = R(e\backslash q)R(r)R(e\backslash qr)^{-1}$, and $L_e(q,r) = L(q/e)L(r)L(rq/e)^{-1}$
- $U(Q;\mathbf{V})_e$ will act on the fiber $p^{-1}\{e\}$ in a split extension $p : E \to Q$.

Universal stabilizers

- $U(Q;\mathbf{V})$ also acts transitively on Q, so for any $e \in Q$, define $U(Q;\mathbf{V})_e$ to be the *universal stabilizer of Q in* $\mathbf{V}$.

$$\begin{tikzcd}
 & rq & \\
e \arrow[ur, "L(rq/e)"] \arrow[rr, bend left, "L(q/e)"] \arrow[rr, bend right, "R(e\backslash q)"'] \arrow[dr, "R(e\backslash qr)"'] & & q \arrow[ul, "L(r)"'] \arrow[dl, "R(r)"] \\
 & qr &
\end{tikzcd}$$

- Define $T_e(q) = R(e\backslash q)L(q/e)^{-1}$, $R_e(q,r) = R(e\backslash q)R(r)R(e\backslash qr)^{-1}$, and $L_e(q,r) = L(q/e)L(r)L(rq/e)^{-1}$
- $U(Q;\mathbf{V})_e$ will act on the fiber $p^{-1}\{e\}$ in a split extension $p : E \to Q$.

Universal stabilizers

- $U(Q;\mathbf{V})$ also acts transitively on Q, so for any $e \in Q$, define $U(Q;\mathbf{V})_e$ to be the *universal stabilizer of Q in $\mathbf{V}$*.

$$
\begin{tikzcd}
 & rq & \\
e \arrow[ur, "L(rq/e)"] \arrow[rr, bend left, "L(q/e)"] \arrow[rr, bend right, "R(e\backslash q)"'] \arrow[dr, "R(e\backslash qr)"'] & & q \arrow[ul, "L(r)"'] \arrow[dl, "R(r)"] \\
 & qr &
\end{tikzcd}
$$

- Define $T_e(q) = R(e\backslash q)L(q/e)^{-1}$, $R_e(q,r) = R(e\backslash q)R(r)R(e\backslash qr)^{-1}$, and $L_e(q,r) = L(q/e)L(r)L(rq/e)^{-1}$
- $U(Q;\mathbf{V})_e$ will act on the fiber $p^{-1}\{e\}$ in a split extension $p : E \to Q$.

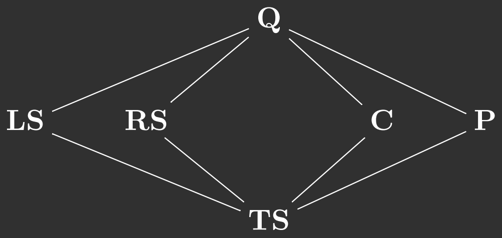
Universal stabilizers

- $U(Q;\mathbf{V})$ also acts transitively on Q, so for any $e \in Q$, define $U(Q;\mathbf{V})_e$ to be the *universal stabilizer of Q in $\mathbf{V}$*.

$$\begin{tikzcd}
 & rq & \\
e \arrow[ur, bend left, "L(rq/e)"] \arrow[rr, bend left=15, "L(q/e)"] \arrow[rr, bend right=15, "R(e\backslash q)"'] \arrow[dr, bend right, "R(e\backslash qr)"'] & & q \arrow[ul, bend right, "L(r)"'] \arrow[dl, bend left, "R(r)"] \\
 & qr &
\end{tikzcd}$$

- Define $T_e(q) = R(e\backslash q)L(q/e)^{-1}$, $R_e(q,r) = R(e\backslash q)R(r)R(e\backslash qr)^{-1}$, and $L_e(q,r) = L(q/e)L(r)L(rq/e)^{-1}$
- $U(Q;\mathbf{V})_e$ will act on the fiber $p^{-1}\{e\}$ in a split extension $p : E \to Q$.

H-symmetry classes



Linear quasigroup theory

H-symmetry: modules as models

- $\mathbf{Q}$: $\mathbb{Z}\langle R, L\rangle$-modules
  - $x \cdot y = x^R + y^L$, $x/y = x^{R^{-1}} - y^{LR^{-1}}$, $x\backslash y = y^{L^{-1}} - x^{RL^{-1}}$
- $\mathbf{C}(xy = yx)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = (x + y)^R$, $x/y = x^{R^{-1}} - y$, $x\backslash y = y^{R^{-1}} - x$
- $\mathbf{LS}(y \cdot yx = x)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = x^R - y = x\backslash y$, $x/y = (x + y)^{R^{-1}}$,
- $\mathbf{P}(y \cdot xy = x)$: $\mathbb{Z}[R]/(R^3 + 1)$-modules
  - $x \cdot y = x^R + y^{R^{-1}}$, $x/y = x^{R^{-1}} + y^R = x\backslash y$
- $\mathbf{TS}$: $\mathbb{Z}$-modules
  - $x \cdot y = x/y = x\backslash y = -(x + y)$

H-symmetry: modules as models

- $\mathbf{Q}$: $\mathbb{Z}\langle R, L\rangle$-modules
  - $x \cdot y = x^R + y^L$, $x/y = x^{R^{-1}} - y^{LR^{-1}}$, $x\backslash y = y^{L^{-1}} - x^{RL^{-1}}$
- $\mathbf{C}(xy = yx)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = (x+y)^R$, $x/y = x^{R^{-1}} - y$, $x\backslash y = y^{R^{-1}} - x$
- $\mathbf{LS}(y \cdot yx = x)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = x^R - y = x\backslash y$, $x/y = (x+y)^{R^{-1}}$,
- $\mathbf{P}(y \cdot xy = x)$: $\mathbb{Z}[R]/(R^3+1)$-modules
  - $x \cdot y = x^R + y^{R^{-1}}$, $x/y = x^{R^{-1}} + y^R = x\backslash y$
- $\mathbf{TS}$: $\mathbb{Z}$-modules
  - $x \cdot y = x/y = x\backslash y = -(x+y)$

H-symmetry: modules as models

- $\mathbf{Q}$: $\mathbb{Z}\langle R, L\rangle$-modules
  - $x \cdot y = x^R + y^L$, $x/y = x^{R^{-1}} - y^{LR^{-1}}$, $x\backslash y = y^{L^{-1}} - x^{RL^{-1}}$
- $\mathbf{C}(xy = yx)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = (x+y)^R$, $x/y = x^{R^{-1}} - y$, $x\backslash y = y^{R^{-1}} - x$
- $\mathbf{LS}(y \cdot yx = x)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = x^R - y = x\backslash y$, $x/y = (x+y)^{R^{-1}}$,
- $\mathbf{P}(y \cdot xy = x)$: $\mathbb{Z}[R]/(R^3+1)$-modules
  - $x \cdot y = x^R + y^{R^{-1}}$, $x/y = x^{R^{-1}} + y^R = x\backslash y$
- $\mathbf{TS}$: $\mathbb{Z}$-modules
  - $x \cdot y = x/y = x\backslash y = -(x+y)$

H-symmetry: modules as models

- $\mathbf{Q}$: $\mathbb{Z}\langle R, L\rangle$-modules
  - $x \cdot y = x^R + y^L$, $x/y = x^{R^{-1}} - y^{LR^{-1}}$, $x\backslash y = y^{L^{-1}} - x^{RL^{-1}}$
- $\mathbf{C}(xy = yx)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = (x+y)^R$, $x/y = x^{R^{-1}} - y$, $x\backslash y = y^{R^{-1}} - x$
- $\mathbf{LS}(y \cdot yx = x)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = x^R - y = x\backslash y$, $x/y = (x+y)^{R^{-1}}$,
- $\mathbf{P}(y \cdot xy = x)$: $\mathbb{Z}[R]/(R^3+1)$-modules
  - $x \cdot y = x^R + y^{R^{-1}}$, $x/y = x^{R^{-1}} + y^R = x\backslash y$
- $\mathbf{TS}$: $\mathbb{Z}$-modules
  - $x \cdot y = x/y = x\backslash y = -(x+y)$

H-symmetry: modules as models

- $\mathbf{Q}$: $\mathbb{Z}\langle R, L\rangle$-modules
  - $x \cdot y = x^R + y^L$, $x/y = x^{R^{-1}} - y^{LR^{-1}}$, $x\backslash y = y^{L^{-1}} - x^{RL^{-1}}$
- $\mathbf{C}(xy = yx)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = (x+y)^R$, $x/y = x^{R^{-1}} - y$, $x\backslash y = y^{R^{-1}} - x$
- $\mathbf{LS}(y \cdot yx = x)$: $\mathbb{Z}[R^{\pm 1}]$-modules
  - $x \cdot y = x^R - y = x\backslash y$, $x/y = (x+y)^{R^{-1}}$,
- $\mathbf{P}(y \cdot xy = x)$: $\mathbb{Z}[R]/(R^3+1)$-modules
  - $x \cdot y = x^R + y^{R^{-1}}$, $x/y = x^{R^{-1}} + y^R = x\backslash y$
- $\mathbf{TS}$: $\mathbb{Z}$-modules
  - $x \cdot y = x/y = x\backslash y = -(x+y)$

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m,q)(n,r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathrm{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q;\mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q;\mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m, q)(n, r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathrm{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q; \mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q; \mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m,q)(n,r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathrm{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q;\mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q;\mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m,q)(n,r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathsf{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q;\mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q;\mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m, q)(n, r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathrm{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q; \mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q; \mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m,q)(n,r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathrm{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q;\mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q;\mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m,q)(n,r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathrm{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q;\mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q;\mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Smith's quasigroup module theory

Just as in group theory, quasigroup module theory can be done in terms of split extensions $E = M \rtimes Q$: $(m,q)(n,r) = (m^{R(r)} + n^{L(q)}, qr)$.

- These come from abelian groups in $\mathbf{V}/Q$: $(p : E \to Q, +, -, 0)$.
  - The abelian group M is defined on a fiber $E_e = \{x \in E \mid (x)p = e\}$.
  - $0 : Q \to E$ injects, so $E \cong_{\mathbf{Set}} E_e \times \mathrm{Im}(Q) \cong_{\mathbf{Set}} E_e \times Q$.
  - Fix $e \in Q$, and E_e is invariant under $U(Q;\mathbf{V})_e$-action.
  - The multiplication of E does not a priori situate E and M in $\mathbf{V}$.
- In order to situate E in $\mathbf{V}$, take identities that define the variety, "linearize them," and mod $\mathbb{Z}U(Q;\mathbf{V})_e$ by their difference.
  - Call this ring $\mathbb{Z}\mathbf{V}Q$. Modules over $\mathbb{Z}\mathbf{V}Q$ are equivalent to abelian groups in $\mathbf{V}/Q$.

Modules over Mendelsohn triple systems

$U(Q;\mathbf{MTS})$

- Because semisymmetry is equivalent to $L(q) = R(q)^{-1}$, $U(Q;\mathbf{MTS})$ is free over $R(Q)$.
  - This is Theorem 3.1.8.
- The universal stabilizer $U(Q;\mathbf{MTS})_e$ is free over

$$\{R_e(e,e), R_e(q,r), T_e(q) \mid (q,r) \in Q^{\#} \times Q, qr \neq e\}.$$

  - This is Remark 3.2.4.
  - If $|Q| = n < \infty$, then $\operatorname{rank}(U(Q;\mathbf{MTS})_e) = n^2 - n + 1$.

$U(Q;\mathbf{MTS})$

- Because semisymmetry is equivalent to $L(q) = R(q)^{-1}$, $U(Q;\mathbf{MTS})$ is free over $R(Q)$.
  - This is Theorem 3.1.8.
- The universal stabilizer $U(Q;\mathbf{MTS})_e$ is free over

$$\{R_e(e,e), R_e(q,r), T_e(q) \mid (q,r) \in Q^{\#} \times Q, qr \neq e\}.$$

  - This is Remark 3.2.4.
  - If $|Q| = n < \infty$, then $\mathrm{rank}(U(Q;\mathbf{MTS})_e) = n^2 - n + 1$.

$U(Q;\mathbf{MTS})$

- Because semisymmetry is equivalent to $L(q) = R(q)^{-1}$, $U(Q;\mathbf{MTS})$ is free over $R(Q)$.
  - This is Theorem 3.1.8.
- The universal stabilizer $U(Q;\mathbf{MTS})_e$ is free over

$$\{R_e(e,e), R_e(q,r), T_e(q) \mid (q,r) \in Q^{\#} \times Q, qr \neq e\}.$$

  - This is Remark 3.2.4.
  - If $|Q| = n < \infty$, then $\mathrm{rank}(U(Q;\mathbf{MTS})_e) = n^2 - n + 1$.

Linearization of MTS identities

- $\frac{\partial(yx\cdot y)}{\partial y} = R(x)R(y) + R(yx)^{-1}$ and $\frac{\partial x}{\partial y} = 0$
  - $J = \left(R(ye)\left(R(x)R(y) + R(yx)^{-1} - 0\right)R(xe)^{-1}\right)$
  - $\mathbb{Z}\mathbf{P}Q = \mathbb{Z}G_e/J$
- $\frac{\partial x^2}{\partial x} = R(x) + R(x)^{-1}$ and $\frac{\partial x}{\partial x} = 1$
  - $I = J + \left(R(xe)\left(R(x) + R(x)^{-1} - 1\right)R(xe)^{-1}\right)$
  - $\mathbb{Z}\mathbf{MTS}Q = \mathbb{Z}G_e/I$

Linearization of MTS identities

- $\frac{\partial(yx{\cdot}y)}{\partial y} = R(x)R(y) + R(yx)^{-1}$ and $\frac{\partial x}{\partial y} = 0$
  - $J = \big(R(ye)\,\big(R(x)R(y) + R(yx)^{-1} - 0\big)\,R(xe)^{-1}\big)$
  - $\mathbb{Z}\mathbf{P}Q = \mathbb{Z}G_e/J$
- $\frac{\partial x^2}{\partial x} = R(x) + R(x)^{-1}$ and $\frac{\partial x}{\partial x} = 1$
  - $I = J + \big(R(xe)\,\big(R(x) + R(x)^{-1} - 1\big)\,R(xe)^{-1}\big)$
  - $\mathbb{Z}\mathbf{MTS}Q = \mathbb{Z}G_e/I$

Linearization of MTS identities

- $\frac{\partial(yx\cdot y)}{\partial y} = R(x)R(y) + R(yx)^{-1}$ and $\frac{\partial x}{\partial y} = 0$
  - $J = \left(R(ye)\left(R(x)R(y) + R(yx)^{-1} - 0\right) R(xe)^{-1}\right)$
  - $\mathbb{Z}\mathbf{P}Q = \mathbb{Z}G_e/J$
- $\frac{\partial x^2}{\partial x} = R(x) + R(x)^{-1}$ and $\frac{\partial x}{\partial x} = 1$
  - $I = J + \left(R(xe)\left(R(x) + R(x)^{-1} - 1\right) R(xe)^{-1}\right)$
  - $\mathbb{Z}\mathbf{MTS}Q = \mathbb{Z}G_e/I$

$\mathbb{Z}\mathbf{MTS}Q$

Proposition 3.3.8

Let Q be a finite, nonempty Mendelsohn quasigroup containing the element e, and set $Q^{\#} = Q \smallsetminus \{e\}$. With $(Q, \mathcal{B})$ denoting the MTS associated with the quasigroup structure, use $\mathcal{B}^{\#}$ to denote the set of blocks in $\mathcal{B}$ not containing the point e. Consider

$$X_1 = \{R_e(x,x)^2 - R_e(x,x) + 1 \mid x \in Q\}$$
$$X_2 = \{R_e(x,e)T_e(xe) + 1 \mid x \in Q^{\#}\}$$
$$X_3 = \{R_e(x,y)R_e(xy,x)R_e(y,xy) + 1 \mid (x\ y\ xy) \in \mathcal{B}^{\#}\},$$

subsets of $\mathbb{Z}U(Q;\mathbf{MTS})_e$. Then $\mathbb{Z}\mathbf{MTS}Q$ is the quotient of the free group of rank $n^2 - n + 1$ by the ideal generated by $X_1 \cup X_2 \cup X_3$.

$\mathbb{Z}\mathbf{MTS}Q$, abstractly

Theorem 3.3.9

Let Q be a nonempty, semisymmetric, idempotent quasigroup, with associated MTS $(Q, \mathcal{B})$. Define $\mathcal{B}^{\#}$ to be the set of all blocks not containing e. Then $\mathbb{Z}\mathbf{MTS}Q$ is isomorphic to the free product

$$\coprod_{Q} \mathbb{Z}[\zeta] * \coprod_{Q^{\#}} \mathbb{Z}\langle x \rangle * \coprod_{\mathcal{B}^{\#}} \mathbb{Z}\langle x, y \rangle, \tag{1}$$

where $\mathbb{Z}[\zeta] = \mathbb{Z}[X]/(X^2 - X + 1)$ is the ring of Eisenstein integers.

Abelian groups in $\mathbf{MTS}$

The Eisenstein integers

- The *Eisenstein integers* have presentation $\mathbb{Z}[X]/(X^2 - X + 1) \cong \mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}$, where $\zeta = e^{\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2} i$.
- Under $v : a + b\zeta \mapsto a^2 + ab + b^2$, $\mathbb{Z}[\zeta]$ is a Euclidean domain (PID... nice!)

A finite $\mathbb{Z}[\zeta]$-module M is isomorphic to a direct sum

$$\bigoplus_{i=1}^{n} \mathbb{Z}[\zeta]/(\pi_i^{r_i}),$$

where each π_i is prime in $\mathbb{Z}[\zeta]$. The elementary divisors of M, $\pi_1^{r_1}, \ldots, \pi_m^{r_m}$, are unique, up to multiplication by units.

The Eisenstein integers

- The *Eisenstein integers* have presentation $\mathbb{Z}[X]/(X^2 - X + 1) \cong \mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}$, where $\zeta = e^{\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$.
- Under $\upsilon : a + b\zeta \mapsto a^2 + ab + b^2$, $\mathbb{Z}[\zeta]$ is a Euclidean domain (PID... nice!)

A finite $\mathbb{Z}[\zeta]$-module M is isomorphic to a direct sum

$$\bigoplus_{i=1}^{n} \mathbb{Z}[\zeta]/(\pi_i^{r_i}),$$

where each π_i is prime in $\mathbb{Z}[\zeta]$. The elementary divisors of M, $\pi_1^{r_1}, \ldots, \pi_m^{r_m}$, are unique, up to multiplication by units.

Eisenstein primes

There are three classes of Eisenstein primes. Up to association by units $\{\pm 1, \pm\zeta, \pm\bar{\zeta}\}$, they take the forms

1. π, where $p = \pi\upsilon \equiv 1 \mod 3$ is a *split* prime in $\mathbb{Z}$
   - $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$
2. $p \in \mathbb{Z}$, with $p \equiv 2 \mod 3$, is prime in $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$; call these *inert* primes
   - $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$
3. $1 + \zeta$ makes $3 = (1+\zeta)(1+\bar{\zeta})$ ramified over $\mathbb{Z}[\zeta]$
   - $\mathbb{Z}[\zeta]/((1+\zeta)^{2n}) \cong \mathbb{Z}/_{3^n}[\zeta]$, $\mathbb{Z}[\zeta]/((1+\zeta)^{2n+1}) \cong \mathbb{Z}[X]/(3^{n+1}, 3^n X, X^2 - X + 1)$

- Call affine MTS of order coprime to 3 *affine, non-ramified* (ANR).

Eisenstein primes

There are three classes of Eisenstein primes. Up to association by units $\{\pm 1, \pm\zeta, \pm\bar{\zeta}\}$, they take the forms

1. π, where $p = \pi\upsilon \equiv 1 \mod 3$ is a *split* prime in $\mathbb{Z}$
   - $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$
2. $p \in \mathbb{Z}$, with $p \equiv 2 \mod 3$, is prime in $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$; call these *inert* primes
   - $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$
3. $1+\zeta$ makes $3 = (1+\zeta)(1+\bar{\zeta})$ ramified over $\mathbb{Z}[\zeta]$
   - $\mathbb{Z}[\zeta]/((1+\zeta)^{2n}) \cong \mathbb{Z}/_{3^n}[\zeta]$,
     $\mathbb{Z}[\zeta]/((1+\zeta)^{2n+1}) \cong \mathbb{Z}[X]/(3^{n+1}, 3^n X, X^2 - X + 1)$

- Call affine MTS of order coprime to 3 *affine, non-ramified* (ANR).

Eisenstein primes

There are three classes of Eisenstein primes. Up to association by units $\{\pm 1, \pm\zeta, \pm\bar{\zeta}\}$, they take the forms

1. π, where $p = \pi\upsilon \equiv 1 \mod 3$ is a *split* prime in $\mathbb{Z}$
   - $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$
2. $p \in \mathbb{Z}$, with $p \equiv 2 \mod 3$, is prime in $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$; call these *inert* primes
   - $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$
3. $1+\zeta$ makes $3 = (1+\zeta)(1+\bar{\zeta})$ ramified over $\mathbb{Z}[\zeta]$
   - $\mathbb{Z}[\zeta]/((1+\zeta)^{2n}) \cong \mathbb{Z}/_{3^n}[\zeta]$,
     $\mathbb{Z}[\zeta]/((1+\zeta)^{2n+1}) \cong \mathbb{Z}[X]/(3^{n+1}, 3^n X, X^2 - X + 1)$

- Call affine MTS of order coprime to 3 *affine, non-ramified* (ANR).

Eisenstein primes

There are three classes of Eisenstein primes. Up to association by units $\{\pm 1, \pm\zeta, \pm\bar{\zeta}\}$, they take the forms

1. π, where $p = \pi\upsilon \equiv 1 \mod 3$ is a *split* prime in $\mathbb{Z}$
   - $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$
2. $p \in \mathbb{Z}$, with $p \equiv 2 \mod 3$, is prime in $\mathbb{Z}$ and $\mathbb{Z}[\zeta]$; call these *inert* primes
   - $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$
3. $1+\zeta$ makes $3 = (1+\zeta)(1+\bar{\zeta})$ ramified over $\mathbb{Z}[\zeta]$
   - $\mathbb{Z}[\zeta]/((1+\zeta)^{2n}) \cong \mathbb{Z}/_{3^n}[\zeta]$,
     $\mathbb{Z}[\zeta]/((1+\zeta)^{2n+1}) \cong \mathbb{Z}[X]/(3^{n+1}, 3^n X, X^2 - X + 1)$

- Call affine MTS of order coprime to 3 *affine, non-ramified* (ANR).

A structure theorem for affine MTS

Theorem not in current draft (close to Thm. 4.4.5)

Every affine MTS has an essentially unique, indecomposable factorization of the form

$$\prod_{i=1}^{n} \mathrm{Aff}(M_i, R_i),$$

where M_i stands for the abelian group structure on $\mathbb{Z}[\zeta]/(\pi_i^{r_i})$, the quotient of $\mathbb{Z}[\zeta]$ by a primary ideal.

- $M \cong N \iff \mathrm{Aff}(M) \cong \mathrm{Aff}(N)$ and $\mathrm{Aff}(M_1 \oplus M_2) \cong \mathrm{Aff}(M_1) \times \mathrm{Aff}(M_2)$
- So now it suffices to describe MTS on $(\mathbb{Z}/_{p^n})$, $(\mathbb{Z}/_{q^n})^2$, $(\mathbb{Z}/_{3^n})^2$, and $\mathbb{Z}/_{3^n} \oplus \mathbb{Z}/_{3^{n+1}}$ ($p \equiv 1 \mod 3$ and $q \equiv 2 \mod 3$).

A structure theorem for affine MTS

Theorem not in current draft (close to Thm. 4.4.5)

Every affine MTS has an essentially unique, indecomposable factorization of the form

$$\prod_{i=1}^{n} \mathsf{Aff}(M_i, R_i),$$

where M_i stands for the abelian group structure on $\mathbb{Z}[\zeta]/(\pi_i^{r_i})$, the quotient of $\mathbb{Z}[\zeta]$ by a primary ideal.

- $M \cong N \iff \mathsf{Aff}(M) \cong \mathsf{Aff}(N)$ and $\mathsf{Aff}(M_1 \oplus M_2) \cong \mathsf{Aff}(M_1) \times \mathsf{Aff}(M_2)$
- So now it suffices to describe MTS on $(\mathbb{Z}/_{p^n})$, $(\mathbb{Z}/_{q^n})^2$, $(\mathbb{Z}/_{3^n})^2$, and $\mathbb{Z}/_{3^n} \oplus \mathbb{Z}/_{3^{n+1}}$ ($p \equiv 1 \mod 3$ and $q \equiv 2 \mod 3$).

Split primes: $1 \mod 3$

- Let $\pi \in \mathbb{Z}[\zeta]$ with $p := \pi \upsilon \equiv 1 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$, so $\mathrm{Aut}(\mathbb{Z}[\zeta]/(\pi^n)) \cong (\mathbb{Z}/_{p^n})^\times$
- $X^2 - X + 1$ has two roots modulo p^n (Donovan et. al., 2015); call them $a^{\pm 1}$.
- $(\mathbb{Z}[\zeta]/(\pi^n), a^{\pm 1})$ are possible MTS isomorphism classes on $\mathbb{Z}[\zeta]/(\pi^n)$.

Split primes: $1 \mod 3$

- Let $\pi \in \mathbb{Z}[\zeta]$ with $p := \pi \upsilon \equiv 1 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$, so $\mathrm{Aut}(\mathbb{Z}[\zeta]/(\pi^n)) \cong (\mathbb{Z}/_{p^n})^\times$
- $X^2 - X + 1$ has two roots modulo p^n (Donovan et. al., 2015); call them $a^{\pm 1}$.
- $(\mathbb{Z}[\zeta]/(\pi^n), a^{\pm 1})$ are possible MTS isomorphism classes on $\mathbb{Z}[\zeta]/(\pi^n)$.

Split primes: $1 \mod 3$

- Let $\pi \in \mathbb{Z}[\zeta]$ with $p := \pi\upsilon \equiv 1 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$, so $\operatorname{Aut}(\mathbb{Z}[\zeta]/(\pi^n)) \cong (\mathbb{Z}/_{p^n})^\times$
- $X^2 - X + 1$ has two roots modulo p^n (Donovan et. al., 2015); call them $a^{\pm 1}$.
- $(\mathbb{Z}[\zeta]/(\pi^n), a^{\pm 1})$ are possible MTS isomorphism classes on $\mathbb{Z}[\zeta]/(\pi^n)$.

Split primes: $1 \mod 3$

- Let $\pi \in \mathbb{Z}[\zeta]$ with $p := \pi\upsilon \equiv 1 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(\pi^n) \cong \mathbb{Z}/_{p^n}$, so $\mathrm{Aut}(\mathbb{Z}[\zeta]/(\pi^n)) \cong (\mathbb{Z}/_{p^n})^\times$
- $X^2 - X + 1$ has two roots modulo p^n (Donovan et. al., 2015); call them $a^{\pm 1}$.
- $(\mathbb{Z}[\zeta]/(\pi^n), a^{\pm 1})$ are possible MTS isomorphism classes on $\mathbb{Z}[\zeta]/(\pi^n)$.

Inert primes: $2 \mod 3$

- Let p be a rational prime congruent to $2 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$, so $\mathrm{Aut}(\mathbb{Z}[\zeta]/(p^n)) \cong \mathrm{GL}_2(\mathbb{Z}/_{p^n})$.
- One isomorphism class on $\mathbb{Z}[\zeta]/(p^n)$; it is given by $\mathrm{Lin}(\mathbb{Z}/_{p^n}[\zeta]) := \mathrm{Lin}((\mathbb{Z}/p^n)^2, T)$, where T is the companion matrix of $X^2 - X + 1$.
- Proof Outline:
  - Suffices to show $\exists v \in (\mathbb{Z}/_{p^n})^2$ so that $(v\ vA)^\top \in \mathrm{GL}_2(\mathbb{Z}/_{p^n})$ (Prokip, 2005) $(*)$.
  - Take the entries of A modulo p, and act on $(\mathbb{Z}/_p)^2$. Because $X^2 - X + 1$ does not split modulo p, $(*)$ holds in the quotient.
  - $\mathbb{Z}/_{p^n}$ is a local ring, so we can use Nakayama's Lemma to lift our basis modulo p to one modulo p^n.

Inert primes: $2 \mod 3$

- Let p be a rational prime congruent to $2 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$, so $\mathrm{Aut}(\mathbb{Z}[\zeta]/(p^n)) \cong \mathrm{GL}_2(\mathbb{Z}/_{p^n})$.
- One isomorphism class on $\mathbb{Z}[\zeta]/(p^n)$; it is given by $\mathrm{Lin}(\mathbb{Z}/_{p^n}[\zeta]) := \mathrm{Lin}((\mathbb{Z}/p^n)^2, T)$, where T is the companion matrix of $X^2 - X + 1$.
- Proof Outline:
  - Suffices to show $\exists v \in (\mathbb{Z}/_{p^n})^2$ so that $(v \; vA)^\top \in \mathrm{GL}_2(\mathbb{Z}/_{p^n})$ (Prokip, 2005) $(*)$.
  - Take the entries of A modulo p, and act on $(\mathbb{Z}/_p)^2$. Because $X^2 - X + 1$ does not split modulo p, $(*)$ holds in the quotient.
  - $\mathbb{Z}/_{p^n}$ is a local ring, so we can use Nakayama's Lemma to lift our basis modulo p to one modulo p^n.

Inert primes: $2 \mod 3$

- Let p be a rational prime congruent to $2 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$, so $\mathsf{Aut}(\mathbb{Z}[\zeta]/(p^n)) \cong \mathsf{GL}_2(\mathbb{Z}/_{p^n})$.
- One isomorphism class on $\mathbb{Z}[\zeta]/(p^n)$; it is given by $\mathsf{Lin}(\mathbb{Z}/_{p^n}[\zeta]) := \mathsf{Lin}((\mathbb{Z}/p^n)^2, T)$, where T is the companion matrix of $X^2 - X + 1$.
- Proof Outline:
    - Suffices to show $\exists v \in (\mathbb{Z}/_{p^n})^2$ so that $(v\ vA)^\top \in \mathsf{GL}_2(\mathbb{Z}/_{p^n})$ (Prokip, 2005) $(*)$.
    - Take the entries of A modulo p, and act on $(\mathbb{Z}/_p)^2$. Because $X^2 - X + 1$ does not split modulo p, $(*)$ holds in the quotient.
    - $\mathbb{Z}/_{p^n}$ is a local ring, so we can use Nakayama's Lemma to lift our basis modulo p to one modulo p^n.

Inert primes: $2 \mod 3$

- Let p be a rational prime congruent to $2 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$, so $\mathsf{Aut}(\mathbb{Z}[\zeta]/(p^n)) \cong \mathsf{GL}_2(\mathbb{Z}/_{p^n})$.
- One isomorphism class on $\mathbb{Z}[\zeta]/(p^n)$; it is given by $\mathsf{Lin}(\mathbb{Z}/_{p^n}[\zeta]) := \mathsf{Lin}((\mathbb{Z}/p^n)^2, T)$, where T is the companion matrix of $X^2 - X + 1$.
- Proof Outline:
  - Suffices to show $\exists v \in (\mathbb{Z}/_{p^n})^2$ so that $(v\ vA)^\top \in \mathsf{GL}_2(\mathbb{Z}/_{p^n})$ (Prokip, 2005) $(*)$.
  - Take the entries of A modulo p, and act on $(\mathbb{Z}/_p)^2$. Because $X^2 - X + 1$ does not split modulo p, $(*)$ holds in the quotient.
  - $\mathbb{Z}/_{p^n}$ is a local ring, so we can use Nakayama's Lemma to lift our basis modulo p to one modulo p^n.

Inert primes: $2 \mod 3$

- Let p be a rational prime congruent to $2 \mod 3$.
- Then $\mathbb{Z}[\zeta]/(p^n) \cong \mathbb{Z}/_{p^n}[\zeta]$, so $\mathsf{Aut}(\mathbb{Z}[\zeta]/(p^n)) \cong \mathsf{GL}_2(\mathbb{Z}/_{p^n})$.
- One isomorphism class on $\mathbb{Z}[\zeta]/(p^n)$; it is given by $\mathsf{Lin}(\mathbb{Z}/_{p^n}[\zeta]) := \mathsf{Lin}((\mathbb{Z}/p^n)^2, T)$, where T is the companion matrix of $X^2 - X + 1$.
- Proof Outline:
  - Suffices to show $\exists v \in (\mathbb{Z}/_{p^n})^2$ so that $(v\ vA)^\top \in \mathsf{GL}_2(\mathbb{Z}/_{p^n})$ (Prokip, 2005) $(*)$.
  - Take the entries of A modulo p, and act on $(\mathbb{Z}/_p)^2$. Because $X^2 - X + 1$ does not split modulo p, $(*)$ holds in the quotient.
  - $\mathbb{Z}/_{p^n}$ is a local ring, so we can use Nakayama's Lemma to lift our basis modulo p to one modulo p^n.

A direct product decomposition theorem

Theorem 4.5.6

Every ANR MTS is isomorphic to a direct product of quasigroups of the form $\text{Lin}(\mathbb{Z}/_{p_1^n}, a^{\pm 1})$ and $\text{Lin}(\mathbb{Z}/_{p_2^n}[\zeta])$ for $p_1 \equiv 1 \mod 3$ and $p_2 \equiv 2 \mod 3$.

Enumeration of ANR MTS

- Denote integer partitions via multisets (X, μ).
- $P(n) =$ number of partitions of n
- $P_E(n) =$ number of partitions consisting of even parts.

Theorem 4.5.7

Let $p \neq 3$ be prime. Then, up to isomorphism, the number of distributive MTS of order p^n is given by

a.) $\displaystyle\sum_{(X,\mu)\vdash n} \sum_{r \in X} (\mu(r)+1)$ whenever $p \equiv 1 \mod 3$;

b.) $P_E(n)$ whenever $p \equiv 2 \mod 3$.

- a.) comes from the fact that $\binom{2+\mu(r)-1}{\mu(r)} = \mu(r)+1$.

Enumeration of ANR MTS

- Denote integer partitions via multisets (X, μ).
- $P(n) =$ number of partitions of n
- $P_E(n) =$ number of partitions consisting of even parts.

Theorem 4.5.7

Let $p \neq 3$ be prime. Then, up to isomorphism, the number of distributive MTS of order p^n is given by

a.) $\displaystyle\sum_{(X,\mu)\vdash n} \sum_{r \in X} (\mu(r) + 1)$ whenever $p \equiv 1 \mod 3$;

b.) $P_E(n)$ whenever $p \equiv 2 \mod 3$.

- a.) comes from the fact that $\binom{2+\mu(r)-1}{\mu(r)} = \mu(r) + 1$.

Enumeration of ANR MTS

- Denote integer partitions via multisets (X, μ).
- $P(n) =$ number of partitions of n
- $P_E(n) =$ number of partitions consisting of even parts.

Theorem 4.5.7

Let $p \neq 3$ be prime. Then, up to isomorphism, the number of distributive MTS of order p^n is given by

a.) $\displaystyle\sum_{(X,\mu)\vdash n} \sum_{r \in X} (\mu(r) + 1)$ whenever $p \equiv 1 \mod 3$;

b.) $P_E(n)$ whenever $p \equiv 2 \mod 3$.

- a.) comes from the fact that $\binom{2+\mu(r)-1}{\mu(r)} = \mu(r) + 1$.

The ramified case

- $\mathbb{Z}[\zeta]/(1+\zeta)^{2k} \cong \mathbb{Z}/_{3^k}[\zeta]$, so even powers work just like inert primes.
- However, $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1} \cong \mathbb{Z}[X]/(X^2-X+1, 3^k X, 3^{k+1}) \cong_{\mathsf{Ab}} \mathbb{Z}/_{3^k} \oplus \mathbb{Z}/_{3^{k+1}}$.
    - Leads to representation theory of mixed congruence classes.
    - However, numerical evidence from the paper of Donovan et. al. seems to indicate that there is only one isomorphism class on each $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1}$.
        - If this is true, then the number of affine MTS of order 3^n is $P(n)$.

The ramified case

- $\mathbb{Z}[\zeta]/(1+\zeta)^{2k} \cong \mathbb{Z}/_{3^k}[\zeta]$, so even powers work just like inert primes.
- However, $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1} \cong \mathbb{Z}[X]/(X^2 - X + 1, 3^k X, 3^{k+1}) \cong_{\mathsf{Ab}} \mathbb{Z}/_{3^k} \oplus \mathbb{Z}/_{3^{k+1}}$.
    - Leads to representation theory of mixed congruence classes.
    - However, numerical evidence from the paper of Donovan et. al. seems to indicate that there is only one isomorphism class on each $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1}$.
        - If this is true, then the number of affine MTS of order 3^n is $P(n)$.

The ramified case

- $\mathbb{Z}[\zeta]/(1+\zeta)^{2k} \cong \mathbb{Z}/_{3^k}[\zeta]$, so even powers work just like inert primes.
- However, $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1} \cong \mathbb{Z}[X]/(X^2 - X + 1, 3^k X, 3^{k+1}) \cong_{\mathsf{Ab}} \mathbb{Z}/_{3^k} \oplus \mathbb{Z}/_{3^{k+1}}$.
    - Leads to representation theory of mixed congruence classes.
    - However, numerical evidence from the paper of Donovan et. al. seems to indicate that there is only one isomorphism class on each $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1}$.
        - If this is true, then the number of affine MTS of order 3^n is $P(n)$.

The ramified case

- $\mathbb{Z}[\zeta]/(1+\zeta)^{2k} \cong \mathbb{Z}/_{3^k}[\zeta]$, so even powers work just like inert primes.
- However, $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1} \cong \mathbb{Z}[X]/(X^2-X+1, 3^k X, 3^{k+1}) \cong_{\mathsf{Ab}} \mathbb{Z}/_{3^k} \oplus \mathbb{Z}/_{3^{k+1}}$.
  - Leads to representation theory of mixed congruence classes.
  - However, numerical evidence from the paper of Donovan et. al. seems to indicate that there is only one isomorphism class on each $\mathbb{Z}[\zeta]/(1+\zeta)^{2k+1}$.
    - If this is true, then the number of affine MTS of order 3^n is $P(n)$.

Lifting the ramified case

- Every matrix representation of ζ over $\mathbb{Z}/_3 \oplus \mathbb{Z}/_9$ and $\mathbb{Z}/_9 \oplus \mathbb{Z}/_{27}$ lifts to one in $\mathsf{SL}_2(\mathbb{Z})$.
- If this holds for all powers of 3, then, then the problem is solved.
- I obtained these lifts through a greedy search, and it may be possible to show that such a search must terminate.

Lifting the ramified case

- Every matrix representation of ζ over $\mathbb{Z}/_3 \oplus \mathbb{Z}/_9$ and $\mathbb{Z}/_9 \oplus \mathbb{Z}/_{27}$ lifts to one in $\mathsf{SL}_2(\mathbb{Z})$.
- If this holds for all powers of 3, then, then the problem is solved.
- I obtained these lifts through a greedy search, and it may be possible to show that such a search must terminate.

Lifting the ramified case

- Every matrix representation of ζ over $\mathbb{Z}/_3 \oplus \mathbb{Z}/_9$ and $\mathbb{Z}/_9 \oplus \mathbb{Z}/_{27}$ lifts to one in $\mathsf{SL}_2(\mathbb{Z})$.
- If this holds for all powers of 3, then, then the problem is solved.
- I obtained these lifts through a greedy search, and it may be possible to show that such a search must terminate.

Beyond set-theoretic triality

Quantum quasigroups

A K-module A, endowed with multiplication $\nabla : A \otimes A \to A$ and comultiplication $\Delta : A \to A \otimes A$ is a *quantum quasigroup* if the *composite maps*

$$\mathsf{G} = (\Delta \otimes 1_A)(1_A \otimes \nabla) \qquad \text{and}$$
$$\Game = (1_A \otimes \Delta)(\nabla \otimes 1_A)$$

are invertible.

- What are some sufficient conditions for obtaining this configuration?

$$\begin{tikzcd}
 & A \arrow[r, leftrightarrow, "(12)"] \arrow[dl, Leftrightarrow, "(23)"'] & A_t \arrow[dr, Leftrightarrow, "(23)"] & \\
A_l \arrow[dr, leftrightarrow, "(12)"'] & & & A_{tl} \arrow[dl, leftrightarrow, "(12)"] \\
 & A_{lt} \arrow[r, Leftrightarrow, "(23)"'] & A_r &
\end{tikzcd}$$

Quantum quasigroups

A K-module A, endowed with multiplication $\nabla : A \otimes A \to A$ and comultiplication $\Delta : A \to A \otimes A$ is a *quantum quasigroup* if the *composite maps*

$$\mathsf{G} = (\Delta \otimes 1_A)(1_A \otimes \nabla) \qquad \text{and}$$
$$\reflectbox{G} = (1_A \otimes \Delta)(\nabla \otimes 1_A)$$

are invertible.

- What are some sufficient conditions for obtaining this configuration?

$$\begin{tikzcd}
 & A \arrow[r, leftrightarrow, "(12)"] & A_t \arrow[dr, Leftrightarrow, "(23)"] & \\
A_l \arrow[ur, Leftrightarrow, "(23)"] \arrow[dr, leftrightarrow, "(12)"'] & & & A_{tl} \arrow[dl, leftrightarrow, "(12)"] \\
 & A_{lt} \arrow[r, Leftrightarrow, "(23)"'] & A_r &
\end{tikzcd}$$

The End