Sylow p-groups of Polynomial Permutations on the Integers mod p^n

Daniel Krenn

(joint work with Sophie Frisch)

Graz University of Technology, Austria

December 21, 2012

DOCTORAL PROGRAM DISCRETE MATHEMATICS
TU & KFU GRAZ·MU LEOBEN AUSTRIA

FWF Der Wissenschaftsfonds.

Supported by the Austrian Science Fund (FWF), project W1230.

Polynomial Functions and Permutations

- p prime (fixed), $n \in \mathbb{N}$
- $f \in \mathbb{Z}[X]$ polynomial

Definition (Polynomial Function)

- function $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ induced by f

- $(F_n, \circ)$ monoid of polynomial functions on $\mathbb{Z}/p^n\mathbb{Z}$ w.r.t. composition

Polynomial Functions and Permutations

- p prime (fixed), $n \in \mathbb{N}$
- $f \in \mathbb{Z}[X]$ polynomial

Definition (Polynomial Function)

- function $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ induced by f

- $(F_n, \circ)$ monoid of polynomial functions on $\mathbb{Z}/p^n\mathbb{Z}$ w.r.t. composition

Definition (Polynomial Permutation)

- polynomial function on $\mathbb{Z}/p^n\mathbb{Z}$ (induce by f) is bijective

- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$ w.r.t. composition

Overview

- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$

Order of Groups

$$|G_1| = p!$$
$$|G_2| = p!(p-1)^p p^p$$
$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)}$$

Overview

- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$

Order of Groups

$$|G_1| = p!$$
$$|G_2| = p!(p-1)^p p^p$$
$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)}$$

Number of Sylow p-groups of G_n

$$(p-1)!(p-1)^{p-2}$$

(if $n \geq 2$)

Overview

- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$

Order of Groups

$$|G_1| = p!$$
$$|G_2| = p!(p-1)^p p^p$$
$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)}$$

Number of Sylow p-groups of G_n

$$(p-1)!(p-1)^{p-2}$$

(if $n \geq 2$)

Sylow p-groups of G_n

- subgroup $C \leq S_p$ cyclic, order p
- $\varphi\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$
- bijective correspondence:

pairs $(C, \overline{\varphi})$

$\leftrightsquigarrow$

Sylow p-groups

(if $n \geq 2$)

Order of Groups

- $(F_n, \circ)$ monoid of polynomial functions on $\mathbb{Z}/p^n\mathbb{Z}$
- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$
- $\beta(k) = \min\left\{n \,\middle|\, p^k \text{ divides } n!\right\}$

Theorem

$$|G_1| = p!$$
$$|G_2| = p!(p-1)^p p^p$$
$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)}$$

Order of Groups

- $(F_n, \circ)$ monoid of polynomial functions on $\mathbb{Z}/p^n\mathbb{Z}$
- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$
- $\beta(k) = \min\left\{n \,\middle|\, p^k \text{ divides } n!\right\}$

Theorem

$$|G_1| = p!$$
$$|G_2| = p!(p-1)^p p^p$$
$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)}$$

- projection $F_n \xleftarrow{\pi_n} F_{n+1}$ has $|\ker \pi_n| = p^{\beta(n+1)}$

Order of Groups

- $(F_n, \circ)$ monoid of polynomial functions on $\mathbb{Z}/p^n\mathbb{Z}$
- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$
- $\beta(k) = \min\left\{n \,\middle|\, p^k \text{ divides } n!\right\}$

Theorem

$$|G_1| = p!$$
$$|G_2| = p!(p-1)^p p^p$$
$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)}$$

- projection $F_n \xleftarrow{\pi_n} F_{n+1}$ has $|\ker \pi_n| = p^{\beta(n+1)}$
- $f \in \mathbb{Z}[X]$, $n \geq 2$:
  - f is permutation on $\mathbb{Z}/p^n\mathbb{Z}$
  - $\iff$
  - f is permutation on $\mathbb{Z}/p\mathbb{Z}$
  - f' has no zero mod p

Sylow p-subgroups

- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$

Theorem (Frisch–K 2011)

- $(p-1)!(p-1)^{p-2}$ *Sylow p-subgroups of* G_n *(if* $n \geq 2$*)*
- *Sylow p-subgroup of* G_n

$$S_{(C,\bar{\varphi})} = \left\{ [f]_{p^n} \in G_n \;\middle|\; [f]_p \in C,\ [f']_p(x) = \frac{\varphi([f]_p(x))}{\varphi(x)} \right\}$$

- *subgroup* $C \leq S_p$ *cyclic, order* p
- $\varphi\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ $\overline{\varphi}$ *class w.r.t. multiplication by constant* $\neq 0$

- *bijective correspondence:*

$$\textit{pairs } (C, \overline{\varphi}) \quad \leftrightsquigarrow \quad \textit{Sylow } p\textit{-subgroups}$$

"Something" in between...

- projective system

$$F_1 \xleftarrow{\pi_1} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \cdots$$

$$G_1 \xleftarrow{\pi_1} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \cdots$$

"Something" in between...

- projective system

$$F_1 \xleftarrow{\psi} E \xleftarrow{\theta} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \cdots$$

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \cdots$$

"Something" in between...

- projective system

$$F_1 \xleftarrow{\psi} E \xleftarrow{\theta} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \cdots$$

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \cdots$$

- $E = \left\{ (f, f') \;\middle|\; \begin{array}{c} f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ f' : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \end{array} \right\}$
- $(f, f') \circ (g, g') = (f \circ g,\ (f' \circ g) \cdot g')$

"Something" in between...

- projective system

$$F_1 \xleftarrow{\psi} E \xleftarrow{\theta} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \cdots$$

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \cdots$$

- $E = \left\{ (f, f') \;\middle|\; \begin{array}{c} f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ f' : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \end{array} \right\}$
- $(f, f') \circ (g, g') = (f \circ g,\ (f' \circ g) \cdot g')$
- $\psi(f, f') = f$
- $\theta([f]_{p^2}) = ([f]_p, [f']_p)$

"Something" in between...

- projective system

$$F_1 \xleftarrow{\psi} E \xleftarrow{\theta} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \cdots$$

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \cdots$$

- $E = \left\{ (f, f') \;\middle|\; \begin{array}{c} f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ f' : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \end{array} \right\}$
- $(f, f') \circ (g, g') = (f \circ g,\ (f' \circ g) \cdot g')$
- $\psi(f, f') = f$
- $\theta([f]_{p^2}) = ([f]_p, [f']_p)$
- $(H, \circ)$ groups of units

"Something" in between...

- projective system

$$F_1 \xleftarrow{\psi} E \xleftarrow{\theta} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \cdots$$

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \cdots$$

- $E = \left\{ (f, f') \;\middle|\; \begin{array}{c} f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \\ f' : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \end{array} \right\}$
- $(f, f') \circ (g, g') = (f \circ g,\ (f' \circ g) \cdot g')$
- $\psi(f, f') = f$
- $\theta([f]_{p^2}) = ([f]_p, [f']_p)$
- $(H, \circ)$ groups of units

Remark

- $\pi_1 = \psi\theta$
- $H = \{(f, f') \in E \mid f \text{ bijective, } f' \text{ has no zero}\}$
- $|H| = p!(p-1)^p$

A Sylow p-subgroup

- group $H = \left\{ (f, f') \in E \;\middle|\; \begin{array}{r} f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ bijective} \\ f' : \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} \end{array} \right\}$

Lemma

- *Sylow p-subgroup of H*

$$S = \left\{ (f, f') \in H \;\middle|\; f \in \langle (0\,1\,2 \ldots p-1) \rangle,\ f' = 1 \right\}$$

A Sylow p-subgroup

- group $H = \left\{ (f, f') \in E \;\middle|\; \begin{array}{c} f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ bijective} \\ f' : \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} \end{array} \right\}$

Lemma

- *Sylow p-subgroup of H*

$$S = \left\{ (f, f') \in H \;\middle|\; f \in \langle (0\,1\,2 \ldots p-1) \rangle,\ f' = 1 \right\}$$

- *normalizer of S in H*

$$N_H(S) = \left\{ (g, g') \in H \;\middle|\; \begin{array}{l} g \in N_H(\langle (0\,1\,2 \ldots p-1) \rangle) \\ g' \text{ constant} \neq 0 \end{array} \right\}$$

A Sylow p-subgroup

- group $H = \left\{ (f, f') \in E \;\middle|\; \begin{array}{r} f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ bijective} \\ f' : \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} \end{array} \right\}$

Lemma

- *Sylow p-subgroup of H*

$$S = \left\{ (f, f') \in H \;\middle|\; f \in \langle (0\,1\,2 \ldots p-1) \rangle,\ f' = 1 \right\}$$

- *normalizer of S in H*

$$N_H(S) = \left\{ (g, g') \in H \;\middle|\; \begin{array}{l} g \in N_H(\langle (0\,1\,2 \ldots p-1) \rangle) \\ g' \text{ constant} \neq 0 \end{array} \right\}$$

$$= \left\{ (g, g') \in H \;\middle|\; \begin{array}{l} \exists k \neq 0\ \forall a, b \colon g(a) - g(b) = k(a-b) \\ g' \text{ constant} \neq 0 \end{array} \right\}$$

A Sylow p-subgroup

- $N_H(S) = \left\{ (g, g') \;\middle|\; \begin{array}{l} \exists k \neq 0 \; \forall a, b \colon g(a) - g(b) = k(a-b) \\ g' \text{ constant} \neq 0 \end{array} \right\}$

Lemma

- $|N_H(S)| = p(p-1)^2$

A Sylow p-subgroup

- $N_H(S) = \left\{ (g, g') \;\middle|\; \begin{array}{l} \exists k \neq 0 \; \forall a, b \colon g(a) - g(b) = k(a-b) \\ g' \text{ constant} \neq 0 \end{array} \right\}$
- $|H| = p!(p-1)^p$

Lemma

- $|N_H(S)| = p(p-1)^2$
- $\mathit{index}\,[H : N_H(S)] = (p-1)!(p-1)^{p-2}$

A Sylow p-subgroup

- $N_H(S) = \left\{ (g, g') \;\middle|\; \begin{array}{l} \exists k \neq 0 \; \forall a, b \colon g(a) - g(b) = k(a-b) \\ g' \text{ constant} \neq 0 \end{array} \right\}$
- $|H| = p!(p-1)^p$

Lemma

- $|N_H(S)| = p(p-1)^2$
- *index* $[H : N_H(S)] = (p-1)!(p-1)^{p-2}$

Corollary

- $(p-1)!(p-1)^{p-2}$ *Sylow p-subgroups of* H

Sylow p-subgroups

- $(G_n, \circ)$ group of polynomial permutations on $\mathbb{Z}/p^n\mathbb{Z}$

Theorem (Frisch–K 2011)

- $(p-1)!(p-1)^{p-2}$ *Sylow p-subgroups of* G_n *(if* $n \geq 2$*)*
- *Sylow p-subgroup of* G_n

$$S_{(C,\bar{\varphi})} = \left\{ [f]_{p^n} \in G_n \;\middle|\; [f]_p \in C,\ [f']_p(x) = \frac{\varphi([f]_p(x))}{\varphi(x)} \right\}$$

- *subgroup* $C \leq S_p$ *cyclic, order* p
- $\varphi\colon \mathbb{Z}/p\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ $\overline{\varphi}$ *class w.r.t. multiplication by constant* $\neq 0$

- *bijective correspondence:*

$$\text{pairs } (C, \overline{\varphi}) \quad \leftrightsquigarrow \quad \text{Sylow } p\text{-subgroups}$$

Open Problem

- C_p cyclic group of order p

Question

Can every finite wreath product

$$C_p \wr C_p \wr \cdots \wr C_p$$

be embedded in G_n for some n?