Coset closure of a circulant S-ring and schurity problem

Ilya Ponomarenko
(based on joint work with S.Evdokimov)

St.Petersburg Department of V.A.Steklov Institute of Mathematics
of the Russian Academy of Sciences

RuFiDiM - Third Russian Finnish Symposium on Discrete Mathematics
15-18 September 2014, Petrozavodsk, Russia

The Schur theorem

Let Γ be a permutation group with a regular subgroup G:

$$\Gamma \leq \mathrm{Sym}(G).$$

The Schur theorem

Let Γ be a permutation group with a regular subgroup G:

$$\Gamma \leq \mathrm{Sym}(G).$$

Let e be the identity of G, Γ_e the stabilizer of e in Γ,

The Schur theorem

Let Γ be a permutation group with a regular subgroup G:

$$\Gamma \leq \mathrm{Sym}(G).$$

Let e be the identity of G, Γ_e the stabilizer of e in Γ, and

$$\mathcal{A} = \mathcal{A}(\Gamma, G) = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathrm{Orb}(\Gamma_e, G)\}$$

where $\underline{X} = \sum_{x \in X} x$.

The Schur theorem

Let Γ be a permutation group with a regular subgroup G:

$$\Gamma \leq \mathrm{Sym}(G).$$

Let e be the identity of G, Γ_e the stabilizer of e in Γ, and

$$\mathcal{A} = \mathcal{A}(\Gamma, G) = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathrm{Orb}(\Gamma_e, G)\}$$

where $\underline{X} = \sum_{x \in X} x$.

Theorem (Schur, 1933)

The module $\mathcal{A}$ is a subring of the group ring $\mathbb{Z}G$.

The Schur theorem

Let Γ be a permutation group with a regular subgroup G:

$$\Gamma \leq \mathrm{Sym}(G).$$

Let e be the identity of G, Γ_e the stabilizer of e in Γ, and

$$\mathcal{A} = \mathcal{A}(\Gamma, G) = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \; X \in \mathrm{Orb}(\Gamma_e, G)\}$$

where $\underline{X} = \sum_{x \in X} x$.

Theorem (Schur, 1933)

The module $\mathcal{A}$ is a subring of the group ring $\mathbb{Z}G$.

Example: $\Gamma_e \leq \mathrm{Aut}(G)$;

The Schur theorem

Let Γ be a permutation group with a regular subgroup G:

$$\Gamma \leq \mathrm{Sym}(G).$$

Let e be the identity of G, Γ_e the stabilizer of e in Γ, and

$$\mathcal{A} = \mathcal{A}(\Gamma, G) = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \; X \in \mathrm{Orb}(\Gamma_e, G)\}$$

where $\underline{X} = \sum_{x \in X} x$.

Theorem (Schur, 1933)

The module $\mathcal{A}$ is a subring of the group ring $\mathbb{Z}G$.

Example: $\Gamma_e \leq \mathrm{Aut}(G)$; in this case the ring $\mathcal{A}$ is called cyclotomic.

Schur rings: definition

Definition

A ring $\mathcal{A} \subset \mathbb{Z}G$ is an S-ring over the group G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of it, such that

Schur rings: definition

Definition

A ring $\mathcal{A} \subset \mathbb{Z}G$ is an S-ring over the group G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of it, such that

1. $\{e\} \in \mathcal{S}$,

Schur rings: definition

Definition

A ring $\mathcal{A} \subset \mathbb{Z}G$ is an S-ring over the group G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of it, such that

1. $\{e\} \in \mathcal{S}$,
2. $X \in \mathcal{S} \;\Rightarrow\; X^{-1} \in \mathcal{S}$,

Schur rings: definition

Definition

A ring $\mathcal{A} \subset \mathbb{Z}G$ is an S-ring over the group G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of it, such that

1. $\{e\} \in \mathcal{S}$,
2. $X \in \mathcal{S} \;\Rightarrow\; X^{-1} \in \mathcal{S}$,
3. $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} :\ X \in \mathcal{S}\}$.

Schur rings: definition

Definition

A ring $\mathcal{A} \subset \mathbb{Z}G$ is an S-ring over the group G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of it, such that

1. $\{e\} \in \mathcal{S}$,
2. $X \in \mathcal{S} \;\Rightarrow\; X^{-1} \in \mathcal{S}$,
3. $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} :\; X \in \mathcal{S}\}$.

Definition

An S-ring $\mathcal{A}$ is called schurian, if $\mathcal{A} = \mathcal{A}(\Gamma, G)$ for some Γ.

Schur rings: definition

Definition

A ring $\mathcal{A} \subset \mathbb{Z}G$ is an S-ring over the group G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of it, such that

1. $\{e\} \in \mathcal{S}$,
2. $X \in \mathcal{S} \ \Rightarrow \ X^{-1} \in \mathcal{S}$,
3. $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathcal{S}\}$.

Definition

An S-ring $\mathcal{A}$ is called schurian, if $\mathcal{A} = \mathcal{A}(\Gamma, G)$ for some Γ.

Wielandt (1966): "*Schur had conjectured for a long time that every S-ring is determined by a suitable permutation group*".

Schur rings: definition

Definition

A ring $\mathcal{A} \subset \mathbb{Z}G$ is an S-ring over the group G, if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of it, such that

1. $\{e\} \in \mathcal{S}$,
2. $X \in \mathcal{S} \ \Rightarrow \ X^{-1} \in \mathcal{S}$,
3. $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathcal{S}\}$.

Definition

An S-ring $\mathcal{A}$ is called schurian, if $\mathcal{A} = \mathcal{A}(\Gamma, G)$ for some Γ.

Wielandt (1966): "*Schur had conjectured for a long time that every S-ring is determined by a suitable permutation group*".

Problem: find a criterion for an S-ring to be schurian.

Circulant S-rings

The schurity problem has sense even for circulant S-rings, i.e. when the underlying group G is cyclic:

Circulant S-rings

The schurity problem has sense even for circulant S-rings, i.e. when the underlying group G is cyclic:

Theorem (Evdokimov-Kovács-P, 2013)

Every S-ring over C_n is schurian if and only if n is of the form:

$$p^k,\ pq^k,\ 2pq^k,\ pqr,\ 2pqr$$

where p, q, r are distinct primes, and $k \geq 0$ is an integer.

Circulant S-rings

The schurity problem has sense even for circulant S-rings, i.e. when the underlying group G is cyclic:

Theorem (Evdokimov-Kovács-P, 2013)

Every S-ring over C_n is schurian if and only if n is of the form:

$$p^k,\ pq^k,\ 2pq^k,\ pqr,\ 2pqr$$

where p, q, r are distinct primes, and $k \geq 0$ is an integer.

An assumption:

The S-ring $\mathcal{A}$ has no sections S of composite order such that $\dim(\mathcal{A}_S) = 2$.

Circulant coset S-rings

Definition

An S-ring $\mathcal{A}$ is called coset, if each $X \in \mathcal{S}$ is of the form $X = xH$ for some group $H \leq G$ such that $\underline{H} \in \mathcal{A}$.

Circulant coset S-rings

Definition

An S-ring $\mathcal{A}$ is called coset, if each $X \in \mathcal{S}$ is of the form $X = xH$ for some group $H \leq G$ such that $\underline{H} \in \mathcal{A}$.

The set of circulant coset S-rings is closed under restrictions, intersections, tensor and wreath products, and consists of schurian rings.

Circulant coset S-rings

Definition

An S-ring $\mathcal{A}$ is called coset, if each $X \in \mathcal{S}$ is of the form $X = xH$ for some group $H \leq G$ such that $\underline{H} \in \mathcal{A}$.

The set of circulant coset S-rings is closed under restrictions, intersections, tensor and wreath products, and consists of schurian rings.

Definition

The coset closure $\mathcal{A}_0$ of a circulant S-ring $\mathcal{A}$ is the intersection of all coset S-rings over G that contain $\mathcal{A}$.

Finding the Schurian closure

Definition

The schurian closure $\mathrm{Sch}(\mathcal{A})$ of an S-ring $\mathcal{A}$ is the intersection of all schurian S-rings over G that contain $\mathcal{A}$.

Finding the Schurian closure

Definition

The schurian closure $\mathrm{Sch}(\mathcal{A})$ of an S-ring $\mathcal{A}$ is the intersection of all schurian S-rings over G that contain $\mathcal{A}$.

Theorem

Let $\mathcal{A}$ be a circulant S-ring and Φ_0 is the group of all algebraic isomorphisms of $\mathcal{A}_0$ that are identical on $\mathcal{A}$. Then

$$\mathrm{Sch}(\mathcal{A}) = (\mathcal{A}_0)^{\Phi_0}.$$

In particular, $\mathcal{A}$ is schurian if and only if $\mathcal{A} = (\mathcal{A}_0)^{\Phi_0}$.

Multipliers

Notation

- $\mathrm{Aut}_{cay}(\mathcal{A}) = \mathrm{Aut}(\mathcal{A}) \cap \mathrm{Aut}(G)$,

Multipliers

Notation

- $\mathrm{Aut}_{cay}(\mathcal{A}) = \mathrm{Aut}(\mathcal{A}) \cap \mathrm{Aut}(G)$,
- $\mathfrak{S}_0$ is the set of all $\mathcal{A}_0$-sections S for which $(\mathcal{A}_0)_S = \mathbb{Z}S$.

Multipliers

Notation

- $\mathrm{Aut}_{cay}(\mathcal{A}) = \mathrm{Aut}(\mathcal{A}) \cap \mathrm{Aut}(G)$,
- $\mathfrak{S}_0$ is the set of all $\mathcal{A}_0$-sections S for which $(\mathcal{A}_0)_S = \mathbb{Z}S$.

Definition

The group $\mathrm{Mult}(\mathcal{A}) \leq \prod_{S \in \mathfrak{S}_0} \mathrm{Aut}_{cay}(\mathcal{A}_S)$ consists of all

$$\Sigma = \{\sigma_S\}_{S \in \mathfrak{S}_0},$$

for which any two automorphisms σ_S and σ_T are compatible

Multipliers

Notation

- $\mathrm{Aut}_{cay}(\mathcal{A}) = \mathrm{Aut}(\mathcal{A}) \cap \mathrm{Aut}(G)$,
- $\mathfrak{S}_0$ is the set of all $\mathcal{A}_0$-sections S for which $(\mathcal{A}_0)_S = \mathbb{Z}S$.

Definition

The group $\mathrm{Mult}(\mathcal{A}) \leq \prod_{S \in \mathfrak{S}_0} \mathrm{Aut}_{cay}(\mathcal{A}_S)$ consists of all

$$\Sigma = \{\sigma_S\}_{S \in \mathfrak{S}_0},$$

for which any two automorphisms σ_S and σ_T are compatible (in particular, they are equal on common subsections of S and T).

Criterion

Theorem

A circulant S-ring $\mathcal{A}$ is schurian if and only if the following two conditions are satisfied for all $S \in \mathfrak{S}_0$:

(1) the S-ring $\mathcal{A}_S$ is cyclotomic,

(2) the homomorphism $\mathrm{Mult}(\mathcal{A}) \to \mathrm{Aut}_{cay}(\mathcal{A}_S)$ is surjective.

Reduction to linear modular system: construction

Let $S_0 \in \mathfrak{S}_0$ and $b \in \mathbb{Z}$ be such that

- b is coprime to $n_{S_0} = |S_0|$,
- the mapping $s \mapsto s^b$, $s \in S_0$, belongs to $\mathrm{Aut}_{cay}(\mathcal{A}_{S_0})$.

Reduction to linear modular system: construction

Let $S_0 \in \mathfrak{S}_0$ and $b \in \mathbb{Z}$ be such that

- b is coprime to $n_{S_0} = |S_0|$,
- the mapping $s \mapsto s^b$, $s \in S_0$, belongs to $\mathrm{Aut}_{cay}(\mathcal{A}_{S_0})$.

Form a system of linear equations in variables $x_S \in \mathbb{Z}$, $S \in \mathfrak{S}_0$:

$$\begin{cases} x_S \equiv x_T \pmod{n_T}, \\ x_{S_0} \equiv b \pmod{n_{S_0}} \end{cases}$$

where $S \in \mathfrak{S}_0$ and $T \preceq S$.

Reduction to linear modular system: construction

Let $S_0 \in \mathfrak{S}_0$ and $b \in \mathbb{Z}$ be such that

- b is coprime to $n_{S_0} = |S_0|$,
- the mapping $s \mapsto s^b$, $s \in S_0$, belongs to $\mathrm{Aut}_{cay}(\mathcal{A}_{S_0})$.

Form a system of linear equations in variables $x_S \in \mathbb{Z}$, $S \in \mathfrak{S}_0$:

$$\begin{cases} x_S \equiv x_T \pmod{n_T}, \\ x_{S_0} \equiv b \pmod{n_{S_0}} \end{cases}$$

where $S \in \mathfrak{S}_0$ and $T \preceq S$.

We are interested only in the solutions of this system that satisfy the additional condition

$$(x_S, n_S) = 1 \quad \text{for all} \quad S \in \mathfrak{S}_0.$$

Reduction to linear modular system: result

Let $\mathcal{A}$ be a circulant S-ring such that for any section $S \in \mathfrak{S}_0$, the S-ring $\mathcal{A}_S$ is cyclotomic.

Reduction to linear modular system: result

Let $\mathcal{A}$ be a circulant S-ring such that for any section $S \in \mathfrak{S}_0$, the S-ring $\mathcal{A}_S$ is cyclotomic.

Theorem

$\mathcal{A}$ is schurian if and only if the above system has a solution for all possible S_0 and b.