Resenhas IME-USP 1996, Vol. 2, No. 3, 303 - 307.

The Congruence Subgroup Theorem and Units of Symmetric Group Rings [1]

G. Leal

Abstract: We work an example that illustrate the strong connection between K-Theory and Group Rings.

Key words: Units of Group Rings, The Congruence subgroup Theorem.

Let K be an algebraic number field and $\mathcal{O}$ its ring of integer. Let $\wp$ be an ideal of $\mathcal{O}$; we denote by π the natural homomorphism

$$SL_n(\mathcal{O}) \longrightarrow SL_n(\mathcal{O}/\wp)$$

The kernel of π, is called the principal $\wp$-congruence subgroup of $SL_n(\mathcal{O})$ and shall be denoted by $\Gamma_\wp$. The subgroups of $SL_n(\mathcal{O})$ that contains some $\Gamma_\wp$ are called *conguence subgroups* and are of finite index in $SL_n(\mathcal{O})$. The converse of this trivial fact is the well known Congruence Subgroup Problem:

Is every subgroup of finite index in $SL_n(\mathcal{O})$ a congruence subgroup?

In general the answer is negative. but in most cases what actually occurs can be precisely described.

In the case where $n = 2$, J.-P. Serre in 1970 [11] and L.N. Vaserštein in 1972 [12] presented a solution in the case where the group of units of $\mathcal{O}$ has infinite order.

Here our concern is the case $n \geq 3$, how it was solved and its relations with the group of units of the integral group rings of finite groups, in particular the symmetric group S_k, $k \in \mathbb{N}$.

In 1965 H. Bass, M. Lazard and J.-P. Serre [1] and J. Mennicke [5] gave a positive solution for the conguence subgroup problem when $\mathcal{O} = \mathbb{Z}$. Finaly, in 1968 H. Bass, J. Milnor and J.-P. Serre [2] presented a complete solution. We extract from this article an outline of the proof.

Let E_{ij} be the matrix with 1 in the ij position and zero elsewhere. Let $E_\wp$ be the normal closure of $\mathcal{E}_\wp =< I+\wp E_{ij} \subset SL_n(\mathcal{O}) | i \neq j >$. We call these generators of $\mathcal{E}_\wp$ *elementary matrices.* Then:

1. Every subgroup of finite index contains some element of $E_\wp$, and $E_\wp$ itself has finite index in $SL_n(\mathcal{O})$. From the fact that $\mathcal{E}_\wp \supseteq E_{\wp^2}$, it follows that $\mathcal{E}_\wp$ is also of finite index in $SL_n(\mathcal{O})$.
2. $E_\wp$ is a congruence subgroup if and only if $E_\wp = \Gamma_\wp$.
3. $\Gamma_\wp$ is generated by $E_\wp$ together with the matrices of the form $\begin{pmatrix} \alpha & 0 \\ 0 & I_{n-2} \end{pmatrix}$ in $\Gamma_\wp$ with $\alpha \in SL_2(\mathcal{O})$.

[1] Research partially supported by CNPq (Brasil).
AMS Classification: QA171, P374.

Define $C_\wp = \frac{\Gamma_\wp}{E_\wp}$. From 1. and 2. we see that $C_\wp$ is finite and that an affirmative answer to the congruence subgroup problem is equivalent to the vanishing of $C_\wp$ for all ideals $\wp$ of $\mathcal{O}$.

Let κ be the natural projection $\Gamma_\wp \to C_\wp$, then every element of $C_\wp$ is of the form $\kappa(\alpha + I_{n-2})$ and, modulo elementary matrices, this element depends only on the first row (a, b) of α. Denoting this image by $\left[\begin{array}{c} b \\ a \end{array}\right]$, we have a surjetive function

$$[\,] : W_q \longrightarrow C_\wp$$

where $W_\wp = \{(a,b) | (a,b) \equiv (1,0) \ mod \, \wp; \ a\mathcal{O} + b\mathcal{O} = \mathcal{O}\}$.

It was discovered by Mennicke in the above article that this function has the following two properties:

M1. $\left[\begin{array}{c} 0 \\ 1 \end{array}\right] = 1$; $\left[\begin{array}{c} b+ta \\ a \end{array}\right] = \left[\begin{array}{c} b \\ a \end{array}\right]$ for all $t \in \wp$; and $\left[\begin{array}{c} b \\ a+tb \end{array}\right] = \left[\begin{array}{c} b \\ a \end{array}\right]$ for all $t \in \mathcal{O}$.

M2. If (a, b_1), $(a, b_2) \in W_\wp$, then $\left[\begin{array}{c} b_1 b_2 \\ a \end{array}\right] = \left[\begin{array}{c} b_1 \\ a \end{array}\right] \left[\begin{array}{c} b_2 \\ a \end{array}\right]$.

We call a function from $W_\wp$ to a group satisfying M1 and M2 a *Mennicke Symbol.*

The first main step was to prove that $C_\wp$ has a presentation with generators $W_\wp$ and relations M1 and M2, so $C_\wp$ depends only on the ring $\mathcal{O}$ and the ideal $\wp$. The solution of the conguence subgroup problem is as follows.

Theorem:

- If K is not totaly imaginary then $C_\wp = \{1\}$.

- If K is totaly imaginary then $C_\wp \cong \mu_r$, where μ_r is the group of the r-roots of units of K and r is a number that depends on the ideal $\wp$.

In a serie of papers, J. Ritter and S.K. Sehgal [6, 7, 8, 9, 10] used this Theorem to produce a finite set of generator for a subgroup of finite index in $\mathcal{U}\mathbb{Z}G$, the group of units of the integral group ring of a group G, for several classes of groups.

Subsequently E. Jespers and G. Leal [3] gave a generalization that we now will apply to the special case of permutations groups.

Let S_k be the symmetric group on k elements and assume $k \geq 5$.

Let $\{e_i | i = 1, 2, \ldots m\}$ be the set of central primitive idempotents of $\mathbb{Q}S_k$. Then

$$\mathbb{Q}S_k = \oplus_{i=1}^m \mathbb{Q}S_k e_i \cong \oplus_{i=1}^m M_{n_i}(\mathbb{Q})$$

and we have the following situation.

$$\begin{tikzcd}
\oplus_{i=1}^{m} M_{n_i}(\mathbb{Z}) \arrow[dd, dash] & \oplus_{i=1}^{m} GL_{n_i}(\mathbb{Z}) \arrow[dd, dash] \arrow[dr, dash] & \\
& & \oplus_{i=1}^{m} SL_{n_i}(\mathbb{Z}) \arrow[dd, dash] \\
\oplus_{i=1}^{m} \mathbb{Z}S_k e_i \arrow[dd, dash] & \oplus_{i=1}^{m} \mathcal{U}\mathbb{Z}S_k e_i \arrow[dd, dash] \arrow[dr, dash] & \\
& & \oplus_{i=1}^{m} \mathcal{U}\mathbb{Z}S_k e_i \cap \oplus_{i=1}^{m} SL_{n_i}(\mathbb{Z}) \arrow[dd, dash] \\
\mathbb{Z}S_k & \mathcal{U}\mathbb{Z}S_k \arrow[dr, dash] & \\
& & \mathcal{U}\mathbb{Z}S_k \cap \oplus_{i=1}^{m} SL_{n_i}(\mathbb{Z})
\end{tikzcd}$$

Note that as $\mathbb{Z}S_k$ and $\oplus_{i=1}^{m} M_{n_i}(\mathbb{Z})$ are orders in $\mathbb{Q}S_k \cong \oplus_{i=1}^{m} M_{n_i}(\mathbb{Q})$ and $GL_1(\mathbb{Z}) = \{\pm 1\}$, all subgroups in the diagram are of finite index.

Assume $e_1 + e_2 = \widehat{A_k} = \dfrac{1}{|A_k|} \displaystyle\sum_{a \in A_k} a$. Then, we have that $\mathbb{Q}S_k e_1 \cong \mathbb{Q}S_k e_2 \cong \mathbb{Q}$ and all other simple components of $\mathbb{Q}S_k$ are isomorphic to $M_n(\mathbb{Q})$ with $n \geq 3$.

Now if A_i is a subgroup of finite index of $\mathcal{U}(\mathbb{Z}S_k e_i)$, then $\times_{i=1}^{m} A_i$ is of finite index in $\mathcal{U}(\times_{i=1}^{m} \mathbb{Z}S_k e_i)$, therefore also in $\times_{i=1}^{m} GL_{n_i}(\mathbb{Z})$.

Recall that for each index $i \geq 3$, we have that $n_i \geq 3$ and that for $i = 1, 2$ the group $\mathcal{U}(\mathbb{Z}S_k e_i)$, is finite.

Now, let a be a transposition in S_k. Define:

$$E = \{1 + (1+a)S_k(1-a), 1 + (1-a)S_k(1+a)\} \subset \mathcal{U}\mathbb{Z}S_k.$$

Note that since $(1+(1+a)x(1-a)) \cdot (1+(1+a)y(1-a)) = 1+(1+a)(x+y)(1-a)$ with $x, y \in S_k$, we have that $\{1+(1+a)\mathbb{Z}S_k(1-a), 1+(1-a)\mathbb{Z}S_k(1+a)\} \subset < E >$.

Hence for each idempotent e_i it follows that

$$\{1 + \alpha(1+a)\mathbb{Z}S_k(1-a) \cdot e_i, 1 + \alpha(1-a)\mathbb{Z}S_k(1+a) \cdot e_i\} \subset < E >,$$

where α is the denominator of e_i. $(\frac{1+a}{2})e_i$ and$(\frac{1-a}{2})e_i$ are noncentral idempotents of $\mathbb{Q}S_k e_i$, $i \geq 3$. Then, up to conjugation, they are matrices of the form:

$$\left[\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right]_{m \times m} \quad \text{and} \quad \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & J \end{array}\right]_{m \times m}$$

where I is the $p \times p$-identity matrix, $p < m$ and J is the $m-p \times m-p$-identity.

The elementary matrices e_{jl} belong to $\mathbb{Q}S_k e_i$, hence for some integer β, we have that $\beta e_{jl} \in \mathbb{Z}S_k e_i$. Therefore, if $j < p$ and $l > p$, we see that

$$4\alpha\beta e_{jl} = 1 + \frac{1+a}{2} 4\alpha\beta e_{jl} \frac{1-a}{2} \in < E > .$$

With the help of the identity $[\gamma e_{ij}, \delta e_{jl}] = \gamma\delta e_{il}$ we can see that $< E >$ contains a congruence subgroup in each noncommutative simple component of $\oplus_{i=1}^m \mathbb{Z}S_k e_i$ so it is of finite index in $\mathbb{Z}S_k$.

The connection between the Congruence Subgroup Theorem and group rings does not stop here, there are many others problems. We list some of them below:

1. What is the index of the subgroup $< E >$, (see[4]).
2. Can this Theorem be proved for group rings?. How can one classify the conguence subgroups of a grup ring?.
3. In connection with the item 3 of our list of facts on elementary matrices, if H is a subgroup of G, is $\mathcal{U}\mathbb{Z}G$ generated by $\mathcal{U}\mathbb{Z}H$ together with E?

References

[1] H. Bass, M. Lazard, J.-P. Serre,*Sous-groupes d'indice fini dans $SL(n,\mathbb{Z})$*, **Bull. Am. Math. Soc. 70** (1964), 385 = 392.

[2] H. Bass, J. Milnor and J.P.-Serre, *Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and $S_{p_{2n}}$ $(n \geq 2)$*, **Publ. Math. I.H.E.S. 33** (1967), 59–137.

[3] E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings*, **Manuscripta Mathematica**, 78 (1993), 303–315.

[4] E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings II*, to appear

[5] J. Mennicke , *Finite Factor Groups of the Unimodular Group*, **Ann. of Math. 81** (1965), 31 -37.

[6] J. Ritter and S.K. Sehgal, *Certain normal subgroups of units in group rings*, **J. Reine Angew. Math.**, 381 (1987), 214–220.

[7] J. Ritter and S.K. Sehgal, *Construction of Units in Integral Group Rings of Finite Nilpotent Groups*, **Trans. Amer. Math. Soc.**, 324 (2)(1991), 603–621.

[8] J. Ritter and S. K. Sehgal, *Generators of Subgroups of $U(\mathbf{Z}G)$*, **Contemp. Math., 93** (1989), 331 - 347.

[9] J. Ritter and S.K. Sehgal, *Construction of units in group rings of monomial and symmetric groups*, **J. Algebra 142** (1991), 511–526.

[10] J. Ritter and S.K. Sehgal, *Units of group rings of solvable and Frobenius groups over large rings of cyclotomic integers*, **J. Algebra**. to appear.

[11] J.-P. Serre, *Le Problem des Groupes de Congruence pour* SL_2, **Ann. of Math. 92** (1970), 389 - 527.

[12] L.N. Vaserstein, *On The Group* SL_2 *Over Dedekind Rings of Arithmetic Type*, **Math. USSR Sbornik**, 18 (1972), 321 - 332.

G. Leal
Instituto de Matemática
Universidade Federal do Rio de Janeiro
Caixa Postal 68530
Rio de Janeiro
gleal@mat.dme.ufrj.br
BRASIL