ACTA ARITHMETICA
XCI.2 (1999)

Some families of finite groups and their rings of invariants

by

Stefan Kühnlein (Karlsruhe)

0. Introduction

0.1. *The general setting.* The theory of polynomial invariants of finite groups is a meeting point of many branches of mathematics such as number theory, combinatorics, mathematical physics, topology and many more. The best-known example is that of the invariants of the symmetric group S_n acting on the polynomial ring in n variables. The ring of invariant polynomials (see below) is generated by the elementary symmetric polynomials, a fact which is frequently used, say, in Galois theory.

In this paper we want to draw attention to a question concerning the mod-p-invariants of subgroups of $\mathrm{GL}(n,\mathbb{Z})$. This can be interpreted as looking at certain families of subgroups of $\mathrm{GL}(n,\mathbb{F}_p)$, one for each prime. How do the degrees of generators of this algebra vary in dependence on p? More concretely, the situation is as follows.

Let R be a commutative unital ring and P an ideal in R. For a subgroup $G \subseteq \mathrm{GL}(n,R)$ we will denote by $(G \bmod P)$ its image under the canonical map to $\mathrm{GL}(n,R/P)$. Sometimes we will omit the brackets in this notation. From now on, all prime ideals under consideration will be non-zero.

The group $(G \bmod P)$ then acts on the free n-dimensional standard module M for R/P and thereby induces an action on the symmetric algebra of the (dual) module of M. We will be interested in the case where R is the ring of integers of an algebraic number field, in which case every non-zero prime ideal is maximal and hence R/P is a field. The symmetric algebra is the polynomial ring in n variables over the field.

If a finite group G acts by automorphisms on a polynomial ring $K[X_1,\ldots,X_n]$, K a field, then we can always choose so-called primary and secondary invariants. Primary invariants are a set of n invariant polynomials which are algebraically independent. They exist by Noether normalisation

1991 *Mathematics Subject Classification*: 13A50, 11F99.

and generate a polynomial algebra. Under this algebra the complete ring of invariants is a finitely generated module. Secondary invariants are module generators for this module under the ring generated by a chosen set of primary invariants. Sometimes the primary invariants are called a homogeneous system of parameters.

All results which we need on invariant theory in general are contained in the very nice account on this subject which was given by Larry Smith in [18]. Occasionally, we will refer to this paper more concretely. The connection with combinatorics is discussed in [20], another overview article which the author highly recommends.

0.2. *The question discussed in this paper.* Let $G \subseteq \mathrm{GL}(n, \mathbb{Z})$ be a subgroup. Then we can look at the reductions $(G \bmod (p))$ for all prime numbers p. To get some idea of what the ring of invariants $\mathbb{F}_p[X_1, \ldots, X_n]^G$ might look like as p varies, one would be very interested in the degrees of generators of this algebra. There are some upper bounds for these degrees, see e.g. [16] for a discussion of this question over the field of complex numbers. But firstly, everything tends to be different in the mod-p-case, and secondly, we would like to deal with all primes simultaneously. The polynomial degree property defined in 2.1 expresses that the degrees of generators grow polynomially in p as p runs through certain subsets of all primes. We will see families of groups which do and families of groups which do not have this property. Finite groups for instance do have the property (see 2.3).

The counterexamples from Section 3 are of interest from another point of view as well. They are groups of units in real quadratic number fields embedded in $\mathrm{SL}(2, \mathbb{Z})$, and the polynomial degree property is more or less equivalent to the question of how the orders of the reduced groups $\mathcal{O}^\times/(\wp \cap \mathcal{O}^\times)$ vary depending on the prime ideal $\wp$. We will study numbers closely related to Lucas numbers. Moreover, the groups under consideration are something like finite counterparts to the groups dealt with in Leopoldt's conjecture.

The problems under consideration are of interest in the calculation of cohomology groups (cf. 1.3, 1.4 as well as [1], [6] or [10] and the references given there). The phenomena which occur are very similar to (and often closely connected with) decomposition of primes in finitely generated number fields. The polynomial degree property which we will introduce in 2.1 and the question whether or not a group does possess this property are related to congruence relations between the matrix entries of the particular group.

1. Some motivating examples. Let us first of all present some well known examples of polynomial invariants in order to proceed to the general

situation we have in mind. If a group G acts on a module, then the invariants of M under G are the set of common eigenvectors with eigenvalue 1 for all group elements. More generally, we might be interested in common eigenvectors for the group elements belonging to some character. We will call such vectors *eigenelements*. We will have no need to consider more general isotypical components (i.e. belonging to irreducible G-modules of higher dimension).

In order to sketch some calculations we state the following

1.1. LEMMA. *Let $\mathcal{G}$ be a group, $\mathcal{H}$ a subgroup in $\mathcal{G}$ of finite index and $\mathcal{A}$ an $\mathcal{R}$-algebra on which $\mathcal{G}$ acts by $\mathcal{R}$-algebra automorphisms. Let $\mu \in \mathcal{A}$ be an eigenelement of $\mathcal{H}$. Then the norm*

$$\mathrm{N}_{\mathcal{G}/\mathcal{H}}(\mu) := \prod_{g \in \mathcal{G}/\mathcal{H}} g\mu$$

is an eigenelement under $\mathcal{G}$ which is well defined up to a unit in $\mathcal{R}$.

The obvious proof is omitted. This procedure is a refinement of the top Chern class of an orbit in [18].

When the ground ring is a field, it is sometimes helpful to calculate the invariants over some larger ground field. Note that this gives the right dimension of the space of invariants.

1.2. EXAMPLE. We will now apply this lemma in the following situation. Fix a power q of some prime number p and denote the field with q elements by $\mathbb{F}_q$. Let $G = \mathrm{SL}(2, \mathbb{F}_q)$ act on $A = \mathbb{F}_q[X, Y]$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) X^e Y^f = (aX + cY)^e (bX + dY)^f$. Look at the following subgroups of G:

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, ac = 1 \right\}, \qquad T := \left\{ \begin{pmatrix} a & -\beta b \\ b & a - \alpha b \end{pmatrix} \,\middle|\, a^2 - \alpha ab + \beta b^2 = 1 \right\},$$

where $\tau^2 + \alpha\tau + \beta \in \mathbb{F}_q[\tau]$ is an irreducible polynomial. When G is viewed as an algebraic group over $\mathbb{F}_q$ then B is a Borel subgroup of G and T is a non-split maximal torus.

B leaves invariant the line $\mathbb{F}_q \cdot X$, and T has an invariant line over the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. Taking norms of these as in Lemma 1.1 we get G-invariant polynomials in A of degrees $q+1$ and q^2-q which turn out to be algebraically independent. The norms are invariant, as there is no non-trivial homomorphism from $\mathrm{SL}(2, \mathbb{F}_q)$ to $\mathbb{F}_q^\times$. As the product of the degrees gives the order of G and G acts faithfully on A we can make use of a result of Kemper (cf. [9] and [18]) which says that under these conditions the algebra A^G is a polynomial algebra generated by the invariants constructed above.

Of course, this is well known since the early 20th century when Dickson calculated the algebra A^G in [2]. For a more modern exposition, cf. [1], [18], or [22].

The phenomenon we want to stress is that we can switch to the following situation: let $\Gamma := \mathrm{SL}(2,\mathbb{Z})$ act on $\mathcal{A} := \mathbb{Z}[X,Y]$ in the obvious way. Then there are two polynomials $f_1, f_2 \in \mathbb{Z}[t]$ such that for every prime p the ring $(\mathcal{A}/p\mathcal{A})^\Gamma$ is generated by two elements of degrees $f_1(p)$ and $f_2(p)$ respectively.

If $\mathcal{O}$ is a ring of integers in a finitely generated number field and if we look at the invariants of $\mathrm{SL}(n,\mathcal{O})$ modulo prime ideals $\wp$, it will be reasonable to partition the primes according to their degrees. If $\wp$ contains the prime number $p \in \mathbb{Z}$ and has index $q = p^d$, then according to Dickson the ring of invariants is generated by polynomials of degrees $p^{dn} - p^{d(n-j)}$, $1 \le j \le n-1$, and one in degree $(p^{dn}-1)/(p^d-1)$. If $\mathcal{O}$ has degree n over $\mathbb{Z}$ then let $\mathcal{P}_i$ be the set of all primes of index p^d in $\mathcal{O}$, $1 \le d \le n$. For every such i there are n polynomials which—evaluated at $p \in \wp$—give the degrees of primary mod-$\wp$-invariants as $\wp$ runs through $\mathcal{P}_i$.

It would not be difficult to incorporate subgroups of $\mathrm{SL}(n,\mathcal{O}_S)$ into the discussion, where $\mathcal{O}_S$ is the ring of S-integers in a number field. In our further exposition, however, we will stick to ordinary rings of integers.

1.3. Example. Let us give another related example which so far seems to be unknown. Let $\Gamma := \mathrm{GL}(2,\mathbb{Z})$. This group acts on binary quadratic forms $\left(\begin{smallmatrix} X & Y \\ Y & Z \end{smallmatrix}\right)$ in the usual way and this defines an action of $\mathrm{PGL}(2,\mathbb{Z})$ on $\mathbb{Z}[X,Y,Z]$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} a^2X + acY + c^2Z \\ 2abX + (ad+bc)Y + 2cdZ \\ b^2X + bdY + d^2Z \end{pmatrix}$$

and extension of this to an algebra isomorphism. Then calculations as above show that for every prime p the ring of invariants mod p is a polynomial algebra generated by three polynomials of degrees 2 (note that $XZ - Y^2$ is the determinant of the quadratic form $\left(\begin{smallmatrix} X & Y \\ Y & Z \end{smallmatrix}\right)$), $p+1$ and $(p^2-p)/2$, so the degrees again are polynomial in p. The dimension of the vector space of homogeneous invariant polynomials of degree n is the number of non-negative integral solutions a, b, c of the equation $2a+(p+1)b+\frac{1}{2}(p^2-p)c = n$.

We mention that the last result can be used to calculate the cohomology of $\mathrm{PGL}(2,\mathbb{Z})$ with coefficients in $\mathbb{F}_p[X,Y,Z]$ for $p \ge 5$. This answers a question I was asked by Jaume Agaude who needs this kind of information for his study of Kac–Moody groups with $\mathrm{PGL}(2,\mathbb{Z})$ as a Weyl group.

To be more precise, let N_n be the homogeneous component of degree n in $\mathbb{Z}[X,Y,Z]$. Multiplication with p gives a short exact sequence of Γ-modules:

$$0 \to N_n \to N_n \to N_n \otimes_{\mathbb{Z}} \mathbb{F}_p \to 0.$$

Call the last module N_n/p. The long exact cohomology sequence for $p \ge 5$

is

$$0 \to H^0(\Gamma, N_n) \to H^0(\Gamma, N_n) \to H^0(\Gamma, N_n/p)$$
$$\to H^1(\Gamma, N_n) \to H^1(\Gamma, N_n) \to H^1(\Gamma, N_n/p) \to 0,$$

because Γ contains a free subgroup of index 12, so all higher cohomology consists of 2- and 3-torsion.

The cohomology of Γ with coefficients in N_n/p is then just H^0 and H^1. The H^0-term is the module of invariants calculated above. The H^1-term comes from the reductions mod p of the integral cohomology. This in turn consists of a free part and of torsion.

The p-torsion part is the image of $H^0(\Gamma, N_n/p)$ in $H^1(\Gamma, N_n)$. This therefore has dimension $\dim(H^0(\Gamma, N_n/p)) - r_0$, where $r_0(n)$ is the rank of $H^0(\Gamma, N_n)$.

The free parts of H^0 and H^1 with coefficients in N_n can be calculated by decomposing $N_n \otimes \mathbb{Q}$ à la Cayley–Sylvester (cf. [19]): We have

$$N_n \otimes \mathbb{Q} \simeq \bigoplus_{j=0}^{[n/2]} M_{2n-4j} \otimes \mathbb{Q},$$

where M_k is the $\mathrm{GL}(2,\mathbb{Z})$-module of all homogeneous polynomials of degree k in two variables. But now we are in a classical situation, and using the Eichler–Shimura isomorphism (cf. [6] or [17]) for H^1 gives the following result.

1.4. Application. *The dimension of $H^i(\mathrm{PGL}(2,\mathbb{Z}),\ N_n/p)$ is as follows. For $i = 0$ it is the number of non-negative integral solutions of the equation $2a + (p+1)b + \frac{1}{2}(p^2-p)c = n$. For $i = 1$ it is this number plus $r_1(n) - r_0(n)$ where*

$$r_0(n) = \begin{cases} 1 & \text{if } n \text{ is even,} \\ 0 & \text{if } n \text{ is odd,} \end{cases}$$

$$\widetilde{r}_1(n) = \begin{cases} \dfrac{[\frac{n}{3}][\frac{n+3}{3}]}{2} + \left[\dfrac{n-2}{6}\right]\left[\dfrac{n+4}{6}\right] & \text{if } n \text{ is even,} \\ (n+2)\left[\dfrac{n+1}{3}\right] - 2\left[\dfrac{n+1}{3}\right]\left[\dfrac{n+4}{3}\right] - \left[\dfrac{n-1}{6}\right]\left[\dfrac{n+5}{6}\right] & \text{if } n \text{ is odd,} \end{cases}$$

$$r_1(n) = \frac{1}{2}\left(\widetilde{r}_1(n) - \left[\frac{n+1}{2}\right]\right). \ \blacksquare$$

If we look at the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{F}_p[X,Y,Z]$ we have to realize that this time the algebras of invariants are no longer polynomial rings but for $p > 2$ they still are uniformly generated by four polynomials of degrees $2, p+1, p(p-1)/2$ and $p(p+1)/2$ (cf. [3]). (Thanks to R. James Shank for pointing out this reference to the author.)

2. The general question. Let $\Gamma \subset \mathrm{GL}(n,\mathbb{C})$ be a group of matrices whose entries lie in the ring of integers $\mathcal{O}$ of a finitely generated number field K. For any prime $\wp \subset \mathcal{O}$, Γ acts on $(\mathcal{O}/\wp)[X_1,\ldots,X_n]$ via the natural action as a subgroup of $\mathrm{GL}(n,\mathcal{O})$.

Motivated by the above examples and being careful at the same time we make the following definition.

2.1. Definition. A subgroup $\Gamma \subseteq \mathrm{GL}(n,\mathcal{O})$ is said to have the *polynomial degree property* if there exists a partition $\mathcal{P}_1,\ldots,\mathcal{P}_k$ of the set of all prime ideals in $\mathcal{O}$ such that for every j, $1 \le j \le k$, there exist polynomials $f_{j,1},\ldots,f_{j,m(j)} \in \mathbb{Q}[t]$ such that for all $\wp \in \mathcal{P}_j$ dividing a prime $p \in \mathbb{Z}$ the algebra $(\mathcal{O}/\wp)[X_1,\ldots,X_n]^\Gamma$ is generated as an $\mathcal{O}/\wp$-algebra by $m(j)$ polynomials of degree $f_{j,1}(p),\ldots,f_{j,m(j)}(p)$, the first n of which are primary invariants and the last ones together with 1 a minimal full set of secondary invariants.

2.2. Remark. Notice that the polynomial degree property is not an intrinsic group theoretic property. It depends on the specified embedding of Γ into $\mathrm{GL}(n,\mathcal{O})$ up to conjugation. It does not depend, however, on the choice of $\mathcal{O}$ because if $\widetilde{\mathcal{O}}$ is the ring of integers in a larger field and $\widetilde{\wp} \subset \widetilde{\mathcal{O}}$ a prime ideal dividing $\wp$ then the Γ-invariants in $(\widetilde{\mathcal{O}}/\widetilde{\wp})[X_1,\ldots,X_n]$ are $(\mathcal{O}/\wp)[X_1,\ldots,X_n]^\Gamma \otimes_{\mathcal{O}/\wp} \widetilde{\mathcal{O}}/\widetilde{\wp}$. (NB: This is the reason for using p in the definition, and not, e.g., the norm of $\wp$.)

If Γ has the polynomial degree property and if the rings of invariants are Cohen–Macaulay for all $\wp$ in an (infinite) equivalence class of the partition, then for these primes the cardinality of $(\Gamma \bmod \wp)$ also has to be polynomial in p. This follows from Proposition 12 in [9] (see also [18], where we find that this cardinality is $\deg(f_{j,1}) \cdot \ldots \cdot \deg(f_{j,n})/(m(j)+1-n)$).

This gives a necessary condition on Γ in case the orders $(\Gamma \bmod \wp)$ should be prime to the characteristic p for almost all $\wp$, because then the invariant rings for these $\wp$ are known to be Cohen–Macaulay (cf. [18] or [8], Theorem 1.6). In the proof of Proposition 3.1, we will see this phenomenon without using the general theorem mentioned above. Compare Proposition 3.4 as well.

2.3. Example. One can easily see that every finite subgroup $G \subseteq \mathrm{GL}(n,\mathcal{O})$ does enjoy the polynomial degree property. If p is larger than $|G|$ then the mod-$\wp$-invariants come from reducing the integral invariants modulo $\wp$—look at the long exact cohomology sequence as in 1.3 and use the fact that higher cohomology of a finite group is $|G|$-torsion.

If p is even larger than $|G|!$ then it is generated by polynomials of degree not larger than $|G|$ (cf. [16] and [18]). Therefore, for $p > |G|!$ there are only finitely many possibilities for the degrees of generators. For the finitely many

primes $< |G|!$ there are also only finitely many possibilities for distributing the degrees of generators.

Gather together those primes $\wp$ for which the degrees coincide. This gives a partition of the set of all primes into finitely many subsets $\mathcal{P}_1, \ldots, \mathcal{P}_k$. On each $\mathcal{P}_i$, the degrees of generators are constant and thereby polynomial in p.

It will usually be very hard to verify the polynomial degree property for specific groups. There are some cases, however, where we can reduce the question to Dickson's results.

2.4. Proposition. *Let $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$ be generated by unipotent elements. Then Γ has the polynomial degree property.*

Proof. We define a partition of the set of primes as follows. $\mathcal{P}_1$ is the set of all primes p for which Γ acts trivially on $\mathbb{F}_p[X,Y]$, $\mathcal{P}_2$ is the set of primes for which Γ acts on $\mathbb{F}_p[X,Y]$ via a non-trivial cyclic quotient, and $\mathcal{P}_3$ is the rest.

If $p \in \mathcal{P}_1$, then $\mathbb{F}_p[X,Y]^\Gamma = \mathbb{F}_p[X,Y]$ is generated by two polynomials of degree 1: $f_{1,1} = f_{1,2} = 1$.

If $p \in \mathcal{P}_2$ we may assume that the quotient of Γ acting on $\mathbb{F}_p[X,Y]$ is generated by $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. We have to calculate the invariants in $\mathbb{F}_p[X,Y]$ under $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. This ring is $\mathbb{F}_p[X, Y(X^{p-1} - Y^{p-1})]$. The polynomials are $f_{2,1} = 1$, $f_{2,2} = t$.

If $p \in \mathcal{P}_3$ we again take one generator of Γ modulo p to be $\gamma_1 := \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. There is a unipotent element in Γ such that its image γ_2 modulo p does not belong to the cyclic group generated by γ_1. Conjugating $\langle \gamma_1, \gamma_2 \rangle$ with something in the normaliser of $\langle \gamma_1 \rangle$ in $\mathrm{GL}(2,\mathbb{F}_p)$ we see that $\langle \gamma_1, \gamma_2 \rangle$ is conjugate to $\langle \gamma_1, \gamma_1^\top \rangle = \mathrm{SL}(2,\mathbb{F}_p)$ (here $\gamma_1^\top$ is the transpose of γ_1) and therefore is $\mathrm{SL}(2,\mathbb{F}_p)$ itself. Now we use the results of Section 1.2: $\mathbb{F}_p[X,Y]^\Gamma$ is generated by polynomials of degree $f_{3,1}(p)$ and $f_{3,2}(p)$, where $f_{3,1} = t+1$ and $f_{3,2} = t^2 - t$. ∎

2.5. Definition/Examples. The group $\Gamma \subseteq \mathrm{GL}(n,\mathcal{O})$ is called *weakly Chinese* if there is a finite subset S of all primes in $\mathcal{O}$ such that for $k \in \mathbb{N}$ and mutually distinct non-zero primes $\wp_1, \ldots, \wp_k \notin S$, the natural map projects Γ surjectively onto $(\Gamma \bmod \wp_1) \times \ldots \times (\Gamma \bmod \wp_k)$.

The groups $\mathrm{SL}(n,\mathcal{O})$ are weakly Chinese, which is a consequence of the Chinese Remainder Theorem (and the fact that the groups $\mathrm{SL}(n,\mathcal{O}/\wp)$ are generated by elementary matrices). A subgroup of $\mathrm{SL}(n,\mathbb{Z})$ which is generated by unipotent elements is weakly Chinese. Finite non-trivial subgroups G of $\mathrm{GL}(n,\mathcal{O})$ are not weakly Chinese: for any two primes which are large enough we will have $G \simeq (G \bmod \wp_1) \simeq (G \bmod \wp_2)$. To be weakly Chinese is not a property of the commensurability class of Γ. For instance, $\mathrm{GL}(n,\mathbb{Z})$ is not weakly Chinese, because every integral matrix has deter-

minant 1 or -1, which remains valid after reducing mod p. In the product $(\mathrm{GL}(n,\mathbb{Z}) \bmod p) \times (\mathrm{GL}(n,\mathbb{Z}) \bmod q)$ for two different odd primes p and q we can choose the determinants independently to be 1 or -1.

2.6. Proposition. *Let $\Gamma \subseteq \mathrm{SL}(n,\mathcal{O})$ be weakly Chinese. Then the following assertions are equivalent*:

(a) *Γ has the polynomial degree property.*

(b) *There is a subgroup of finite index in Γ having the polynomial degree property.*

(c) *Every subgroup in Γ of finite index has the polynomial degree property.*

Proof. As a consequence of the hypothesis, every subgroup of finite index in Γ will have the same image modulo $\wp$ for almost all primes $\wp$. Indeed, let S be as in 2.5. If $\Delta \subseteq \Gamma$ is a subgroup of finite index d, then let $\wp_1, \ldots, \wp_k \notin S$ be primes for which $(\Gamma \bmod \wp) \neq (\Delta \bmod \wp)$.

The group $(\Delta \bmod \wp_1) \times \ldots \times (\Delta \bmod \wp_k)$ has index at most d in $(\Gamma \bmod \wp_1) \times \ldots \times (\Gamma \bmod \wp_k)$. On the other hand, the index is at least 2^k, so $k \leq \log_2 d$. Therefore for all but $|S| + \log_2 d$ primes the reductions of Γ and Δ coincide. As these reductions govern the finite invariants, we are done. ∎

2.7. Corollary. *Every subgroup of finite index in $\mathrm{SL}(n,\mathcal{O})$ has the polynomial degree property.*

Proof. $\mathrm{SL}(n,\mathcal{O})$ is weakly Chinese and has the polynomial degree property. ∎

By 2.6, the example after Definition 2.5 and 2.4 every subgroup of finite index in a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ generated by unipotents has the polynomial degree property.

In Section 3 we will give an example of a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ which is not weakly Chinese. Interestingly, this will turn out not to have the polynomial degree property. It would be important to know whether the polynomial degree property is an invariant of commensurability classes without conditions such as being weakly Chinese, and to know the exact relation between the polynomial degree property and being weakly Chinese.

It is clear from Dickson's results that a group which maps surjectively to almost all $\mathrm{SL}(n,\mathcal{O}/\wp)$ does have the polynomial degree property. Let us give a non-trivial example for these. For this purpose, let $\lambda = (1+\sqrt{5})/2$ be the golden ratio.

We use the two matrices

$$T := \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \qquad S := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The ring $\mathbb{Z}[\lambda]$ is the ring of integers in $\mathbb{Q}(\sqrt{5})$.

2.8. Proposition. *The group $\Gamma = \langle S, T\rangle \subset \mathrm{SL}(2, \mathbb{Z}[\lambda])$ has the polynomial degree property.*

Proof. Let $\mathcal{O} = \mathbb{Z}[\lambda]$. Set $\mathcal{P}_1 := \{(2)\}$, $\mathcal{P}_2 := \{(\sqrt{5})\}$. We do not want to care about these two primes any more.

By tedious matrix multiplications one can show that the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ is contained in the group generated by S and $\widetilde{T} := \left(\begin{smallmatrix}1 & \lambda/2\\ 0 & 1\end{smallmatrix}\right)$. This group therefore projects surjectively to $\mathrm{SL}(2, \mathcal{O}/\wp)$ for every prime not dividing 10. The same of course then holds for our original group Γ, and we may set $\mathcal{P}_3 := \{\wp \mid \wp \text{ divides a decomposed prime}\}$ and $\mathcal{P}_4 := \{\wp \mid \wp \text{ divides an inert prime} \neq 2\}$. On $\mathcal{P}_3$ we may take the polynomials $f_{3,1}(t) = t + 1$ and $f_{3,2}(t) = t^2 - t$, on $\mathcal{P}_4$ the polynomials $f_{4,1}(t) = t^2 + 1$ and $f_{4,2}(t) = t^4 - t^2$. ∎

2.9. Remark. The group Γ from the last proposition is the Hecke group $G(5)$ and in particular the first example of a series of non-arithmetic subgroups of $\mathrm{SL}(2, \mathbb{R})$ which were introduced by Hecke in [7]. It is not known what the set of entries of the matrices from $G(5)$ is. There are some restrictions, in particular there is a restriction modulo 2 (cf. Rosen's paper [15] on λ-continued fractions). It would be interesting to get more information on the entries of $G(5)$. In particular, one would like to check whether or not $G(5)$ satisfies Weyl's asymptotic law on the distribution of eigenvalues of the Laplace operator on Γ-invariant L^2-functions on the upper half plane. This could be attacked if the determinant of the scattering matrix could be calculated (cf. [4] and [13]); here the entries play a vital role, as in principle one has to compute Eisenstein series.

The above proof shows that modulo primes not dividing 2 there are no congruence restrictions on the entries of $G(5)$.

We can embed $\mathrm{SL}(2, \mathcal{O})$ into $\mathrm{SL}(4, \mathbb{Z})$ via restriction of scalars, a possible choice of the image of Γ is given by the group generated by

$$\begin{pmatrix} 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 1\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ -1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

It is not yet known whether this group has the polynomial degree property.

3. Some groups which do not have the polynomial degree property. It is now time to give a series of examples of groups which do not have the polynomial degree property. Let d be a square-free natural number and define $\Gamma_d \subseteq \mathrm{SL}(2, \mathbb{Z})$ by

$$\Gamma_d := \left\{ \begin{pmatrix} a & b\\ bd & a \end{pmatrix} \,\middle|\, a \in \mathbb{N},\ b \in \mathbb{Z} \right\}.$$

Then Γ_d is isomorphic to a subgroup of finite index in the group of totally positive units in the ring of integers $\mathcal{O}_d$ in $\mathbb{Q}(\sqrt{d})$ and therefore infinite cyclic (cf. [23]).

Let us write $\Gamma_d = \langle A \rangle$ for some $A = \left(\begin{smallmatrix} a & b \\ db & a \end{smallmatrix}\right)$. We first want to show that Γ is not weakly Chinese. This will be clear if we know that there are infinitely many primes p_i for which the reduction of A modulo p_i has even order, because then $(\Gamma \bmod p_1) \times \ldots \times (\Gamma \bmod p_k)$ cannot be cyclic. We will show the stronger assertion that there are infinitely many primes p such that A modulo p has order a power of two. For this purpose let $A^{2^e} = \left(\begin{smallmatrix} a_e & b_e \\ db_e & a_e \end{smallmatrix}\right)$, $e \geq 0$. The primes not dividing d modulo which A has order a power of two are exactly the prime divisors of the integers $a_e - 1$, $e \geq 0$. But the recursion formula $a_{e+1} = 2a_e^2 - 1$ immediately implies that the set of these primes is infinite.

3.1. Proposition. *For square-free $d \geq 2$, Γ_d does not have the polynomial degree property.*

Proof. Γ is generated by a matrix A. Let p be a prime number which is unramified in $\mathbb{Q}(\sqrt{d})$. Then A modulo p is diagonalisable at least over $\mathbb{F}_{p^2}$. Let λ, λ^{-1} be its eigenvalues and denote corresponding eigenvectors in $\mathbb{F}_{p^2}X \oplus \mathbb{F}_{p^2}Y$ by U and V. It is then easy to check that $\mathbb{F}_p[X, Y]$ is generated as an algebra by scalar multiples of UV, $U^{\mu(p)}$ and $V^{\mu(p)}$ where $\mu(p)$ denotes the order of A modulo p (scalar multiples to get polynomials over $\mathbb{F}_p$—the quadratic extension $\mathbb{F}_{p^2}$ does no longer play a role then).

Aside: As pointed out in [16], there is always one generator of degree $|G|$ when G is a cyclic group. Take any element of degree 1 and its norm according to Lemma 1.1.

Let $\nu(p) = p - 1$ or $p + 1$ according to whether p is not or is inert. For every p, $\mu(p)$ divides $\nu(p)$. If the polynomial degree property holds for Γ, then there would have to be finitely many equivalence classes $\mathcal{P}_1, \ldots, \mathcal{P}_k$ of primes such that on $\mathcal{P}_j$ the equation $\mu(p) = \nu(p)/n_j$ holds for some $n_j \in \mathbb{N}$. In particular, the function $p \mapsto \nu(p)/\mu(p)$ would have to assume finitely many values only, or equivalently $p \mapsto p/\mu(p)$ would have to be bounded on the set of all primes. There does not seem to be known too much on this function and we therefore give a short proof for its unboundedness.

If $p \mapsto \nu(p)/\mu(p)$ were bounded, we would have finitely many numbers $n_1, \ldots, n_k \in \mathbb{N}$ such that for all but finitely many prime numbers l one of the set $\{n_1 l \pm 1, \ldots, n_k l \pm 1\}$ would have to be a prime. This comes from the fact that almost every prime number l is $\mu(p)$ for some prime p (look at the lth powers of A—this is a very special flavour of our situation). Now choose $2k$ prime numbers $p_1, \ldots, p_{2k}$ which are coprime to $n_1, \ldots, n_k$. The Chinese Remainder Theorem says that the system of linear congruence

equations

$$x \equiv n_i^{-1} \bmod p_i, \qquad 1 \le i \le k,$$
$$x \equiv -n_i^{-1} \bmod p_{k+i}, \qquad 1 \le i \le k,$$

is equivalent to one condition $x \equiv m \bmod (p_1 \cdot \ldots \cdot p_{2k})$. By Dirichlet's Theorem on prime numbers in arithmetic progressions (cf. [12]), this equation has infinitely many prime numbers as solutions. Therefore for infinitely many primes l every element of the set $\{n_1 l \pm 1, \ldots, n_k l \pm 1\}$ is divisible by one of $p_1, \ldots, p_{2k}$.

This contradicts the assumption that Γ_d has the polynomial degree property. ∎

3.2. Remarks. A reasoning similar to the last proof shows that the polynomial degree property would have implied that there is an $n \in \mathbb{N}$ for which infinitely many of the numbers $n \cdot 3^e \pm 1$ are prime. This does not seem to be known. The function $p \mapsto \mu(p)$ is also of interest for calculating mod-p-systems of Hecke eigenvalues in the cohomology of $\mathrm{SL}(2, \mathcal{O}_d)$ (cf. [11]), in particular with respect to the existence of certain Galois representations.

It should be pointed out that the upper left entries of A^n are close relatives of Lucas numbers, the prime factors of which are the object of some interesting studies (cf. [14]).

If $\mathcal{O}$ is a ring of integers of degree n, one can always embed $\mathcal{O}^\times$ into $\mathrm{GL}(n, \mathbb{Z})$. This embedding comes from choosing an integral basis of $\mathcal{O}$ and is well defined up to conjugation. We would like to address the question of whether this group has the polynomial degree property. This is true if the unit group is finite. It does not hold in the real quadratic case and is unknown in all remaining cases. If $S = \{p_1, \ldots, p_n\}$ is a finite set of primes and p some further prime, then a theorem of Chevalley which was improved upon by Grunewald and Segal in [5] says that there are primes $q_1, \ldots, q_m \notin S \cup \{p\}$ such that the kernel of the natural map from Γ to $(\Gamma \bmod q_1) \times \ldots \times (\Gamma \bmod q_m)$ is contained in the kernel of the natural map to $(\Gamma \bmod p)$. This of course means that the natural map from Γ to $(\Gamma \bmod p) \times (\Gamma \bmod q_1) \times \ldots \times (\Gamma \bmod q_m)$ cannot be surjective, so Γ is not weakly Chinese. In this particular case, asking about the polynomial degree property is a complementary question to Leopoldt's conjecture which asks about the p-adic topology of the group of units congruent to 1 modulo every prime dividing p (cf. [21]).

Let us now put this last proposition into a more conceptual frame. To this end, we will need the following lemma.

3.3. Lemma. *Let $\Gamma \subseteq \mathrm{GL}(n, \mathcal{O})$ be a group and assume that there are infinitely many prime ideals $\wp \subset \mathcal{O}$ for which the cardinality $|(\Gamma \bmod \wp)|$ is less than a given constant N. Then Γ is finite of cardinality less than N.*

P r o o f. Let $\gamma_0, \ldots, \gamma_N$ be in Γ. Then for infinitely many prime ideals $\wp$ there exist $i \neq j$ such that $\gamma_i \equiv \gamma_j \pmod{\wp}$. By Dirichlet's pigeonhole principle there are indices $i \neq j$ such that $\gamma_i \equiv \gamma_j \pmod{\wp}$ for infinitely many $\wp$. Clearly this implies $\gamma_i = \gamma_j$ and Γ cannot have more than N elements. ∎

It is not true that $\Gamma \subset \Delta \subset \mathrm{SL}(n, \mathcal{O})$ and $[\Delta \bmod \wp : \Gamma \bmod \wp] \leq N$ for all $\wp$ implies $[\Delta : \Gamma] \leq N$. The index does not even have to be finite. For example, remember the Hecke group $G(5)$ from Proposition 2.8. It has infinite index in $\mathrm{SL}(2, \mathbb{Z}[(1+\sqrt{5})/2])$ yet the reductions coincide for almost all primes $\wp$. Another famous example is the normal closure of $\left(\begin{smallmatrix} 1 & 6 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{SL}(2, \mathbb{Z})$ which also has infinite index but the same reductions away from 2 and 3.

3.4. Proposition. *Let $\Gamma \subset \mathrm{GL}(n, \mathcal{O})$ be infinite and let $\wp_1, \wp_2, \ldots$ be a sequence of prime ideals such that (if p_i is the rational prime inside $\wp_i$) we have*

$$\lim_{i \to \infty} \frac{|\Gamma \bmod \wp_i|}{p_i} = 0.$$

Then Γ does not have the polynomial degree property.

P r o o f. For almost all i the ring $(\mathcal{O}/\wp_i[X_1, \ldots, X_n])^{\Gamma}$ is Cohen–Macaulay, because $|\Gamma \bmod \wp_i|$ is coprime to p_i. Assume Γ has the polynomial degree property.

As stated in Remark 2.2 it would then follow that there is a polynomial F such that for infinitely many $\wp_i$, the cardinality is $|\Gamma \bmod \wp_i| = F(p_i)$. Because of the hypothesis this polynomial must be constant, whence Lemma 3.3 implies that Γ is finite. ∎

3.5. *Final questions.* It is an interesting fact that the non-finite examples for which the polynomial degree property is known to hold are of modular type, i.e. for almost all p the cardinality of Γ modulo p is divisible by p. For the groups Γ_d above this is never the case. This modularity is equivalent to the fact that for almost all p, Γ mod p contains unipotent elements. This does not imply that Γ contains unipotents. Nevertheless, we would like to know whether in the converse direction an analogue of Proposition 2.4 holds for subgroups of $\mathrm{GL}(n, \mathbb{Z})$, $n \geq 3$.

Is there a description of the set of groups having the polynomial degree property which does not use invariant theory? A possible candidate for this might be a variant of the property to be weakly Chinese which takes care of finite subgroups. The only groups for which the author can verify the polynomial degree property are finite groups, weakly Chinese groups, and some combinations of these.

With respect to Remark 2.9: is the polynomial degree property invariant under restriction of scalars?

Are there reasonable generalisations of the polynomial degree property to higher cohomology?

References

[1] A. Adem and R. J. Milgram, *Cohomology of Finite Groups*, Springer, Berlin, 1994.

[2] L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc. 12 (1911), 75–98.

[3] —, *On invariants and the theory of numbers*, The Madison Colloquium, 1913; repr. Dover, 1966.

[4] J. Elstrodt, F. Grunewald and J. Mennicke, *Groups Acting on Hyperbolic Space*, Springer, Berlin, 1997.

[5] F. Grunewald and D. Segal, *On congruence topologies in number fields*, J. Reine Angew. Math. 311/312 (1979), 389–396.

[6] K. Haberland, *Perioden für Modulformen einer Variablen und Gruppencohomologie I*, *II*, *III*, Math. Nachr. 112 (1983), 245–315.

[7] E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung*, Math. Ann. 112 (1936), 664–699; also in: Mathematische Werke, Göttingen, 1959, 591–626.

[8] M. Hochster and J. A. Eagon, *Cohen–Macaulay rings*, *invariant theory*, *and the generic perfection of determinantal loci*, Amer. J. Math. 93 (1971), 1020–1058.

[9] G. Kemper, *Calculating invariant rings of finite groups over arbitrary fields*, J. Symbolic Comput. 21 (1996), 351–366.

[10] S. Kühnlein, *Kohomologie spezieller S-arithmetischer Gruppen und Modulformen*, Bonner Math. Schriften 264 (1994).

[11] —, *Torsion classes in cohomology and Galois representations*, J. Number Theory 70 (1998), 184–190.

[12] S. Lang, *Algebraic Number Theory*, Springer, Berlin, 1993.

[13] P. D. Lax and R. S. Phillips, *Scattering Theory for Automorphic Functions*, Ann. of Math. Stud. 87, Princeton Univ. Press, 1976.

[14] P. Moree and P. Stevenhagen, *Prime divisors of Lucas sequences*, Acta Arith. 82 (1997), 403–410.

[15] D. Rosen, *An arithmetic characterization of the parabolic points of* $G(2\cos\pi/5)$, Glasgow Math. J. 6 (1963), 88–96.

[16] B. J. Schmid, *Finite groups and invariant theory*, in: Séminaire d'Algèbre, P. Dubriel et M. P. Malliavin (eds.), Lecture Notes in Math. 1478, Springer, 1991, 35–66.

[17] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton, 1994.

[18] L. Smith, *Polynomial invariants of finite groups. A survey of recent developments*, Bull. Amer. Math. Soc. 34 (1997), 211–250.

[19] T. Springer, *Invariant Theory*, Lecture Notes in Math. 585, Springer, Heidelberg, 1977.

[20] R. P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. (N.S.) 1 (1979), 475–511.
[21] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.
[22] C. Wilkerson, *A primer on Dickson invariants*, Contemp. Math. 19 (1983), 421–434.
[23] D. Zagier, *Zetafunktionen und quadratische Zahlkörper*, Springer, Berlin, 1981.

Mathematisches Institut II der Universität
D-76128 Karlsruhe, Germany
E-mail: sk@ma2s1.mathematik.uni-karlsruhe.de

Received on 22.9.1998
and in revised form on 3.2.1999 (3468)