PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 4, April 2009, Pages 1169–1173
S 0002-9939(08)09758-X
Article electronically published on November 17, 2008

GRÖBNERIAN DICKSON POLYNOMIALS

MÜFİT SEZER AND ÖZGÜN ÜNLÜ

(Communicated by Bernd Ulrich)

Abstract. Let F be a finite field and k be a positive integer. We compute the reduced Gröbner basis for the Hilbert ideal of $GL_k(F)$ in terms of Dickson invariants of its subgroups.

Introduction

Let F be a finite field with q elements and $GL_k(F)$ be the general linear group of a $k < \infty$ dimensional vector space over F. The ring of invariants of the natural action of $GL_k(F)$ on $R := F[x_1, x_2, \dots, x_k]$ was computed by Dickson [2] and was found to be a polynomial ring on certain polynomials that are called Dickson invariants. Since the Dickson invariants form a homogeneous system of parameters for R, R is a free module over the invariant ring. A nice generating set for R as a module over the invariant ring was given by Campbell et al. [1] and Steinberg [3], where it is shown that there exists a basis for R consisting of monomial factors of a single monomial. An important ingredient of [1] is the study of the Hilbert ideal, which is the ideal in R generated by positive degree invariants. Among other things, Campbell et al. computed the lead term ideal of the Hilbert ideal with respect to lexicographic order and gave an algorithm that produces its reduced Gröbner basis. They also introduced a family of polynomials that approximate this basis; see [1, §§5, 6]. The purpose of this paper is to describe the Gröbner basis in question more explicitly. In fact, we show that for each $1 \leq i \leq k$, the i-th element in the Gröbner basis is a polynomial in the Dickson invariants of $GL_i(F)$, and we compute this polynomial; see Proposition 4. We do this by proving a suitable relation among the Dickson invariants in R.

For a nice account of Dickson invariants we refer the reader to [5], and for a background on the Gröbner basis we recommend [4].

The Gröbner basis

We denote the general linear group $GL_k(F)$ simply by G. We call the ring of invariants which is generated by the Dickson invariants the Dickson algebra and denote it by R^G. The corresponding Hilbert ideal is denoted by $R_+^G \cdot R$. We use the graded lexicographic order with $x_1 < x_2 < x_3 < \cdots < x_k$ on R and the leading monomial of a polynomial f in R will be denoted by $\mathrm{LM}(f)$. For i in $\{1, 2, \dots, k\}$

Received by the editors February 25, 2008.
2000 *Mathematics Subject Classification.* Primary 13A50.
Key words and phrases. Dickson polynomials, Gröbner basis, Hilbert ideal.

we define G_i as the subgroup of G that stabilizes x_j for $i < j \leq k$. In particular $G_k = G$ and $G_0 = 1$. One way to construct the Dickson invariants is via the polynomial

$$f_{x_1,x_2,\dots,x_k}(t) = \prod_{(a_1,a_2,\dots,a_k)\in F^k} (t+a_1x_1+\cdots+a_kx_k) = \sum_{i=0}^{k} d_{k,i}(x_1,\dots,x_k)t^{q^i} \in R[t].$$

Then by [2], $R^G = F[d_{k,i}(x_1,\dots,x_k) \mid 0 \leq i \leq k-1]$ and the invariant polynomials $d_{k,i}(x_1,\dots,x_k)$ for $0 \leq i \leq k-1$ are the celebrated Dickson invariants. Note that the degree of $d_{k,i}(x_1,\dots,x_k)$ is $q^k - q^i$.

More generally, for a positive integer s and polynomials $m_1, m_2, \dots, m_s$ in R we define

$$\begin{aligned} f_{m_1,m_2,\dots,m_s}(t) &= \prod_{(a_1,a_2,\dots,a_s)\in F^s} (t + a_1m_1 + a_2m_2 + \cdots + a_sm_s) \\ &= \sum_{i=0}^{s} d_{s,i}(m_1,\dots,m_s)t^{q^i} \in R[t]. \end{aligned}$$

For s in $\{1,2,\dots,k\}$, instead of $f_{x_1,x_2,\dots,x_s}(t)$ we will simply write $f_s(t)$, and instead of $d_{s,j}(x_1,x_2,\dots,x_s)$ we will write $d_{s,j}$. Then, in our notation, the G_s invariant of the subalgebra $F[x_1,x_2,\dots,x_s]$ is equal to $F[d_{s,0},d_{s,1},\dots,d_{s,s-1}]$. For s in $\{1,2,\dots,k\}$ set

$$g_{s,0} = 1,$$

and for v in $\{1,\dots,k-s+1\}$ define

$$g_{s,v} = -\Big(\sum_{j=0}^{\min\{v-1,s-1\}} d_{s,s-j-1}^{q^{v-1}}\, g_{s,v-j-1}\Big). \tag{1}$$

Note that $g_{s,v}$ is in R^{G_s} for v in $\{1,\dots,k-s+1\}$. For all s in $\{1,2,\dots,k\}$ we further define

$$g_s = -g_{s,k-s+1}.$$

We first compute the leading monomials of $g_{s,v}$ for s in $\{1,2,\dots,k\}$ and v in $\{1,\dots,k-s+1\}$.

Lemma 1. *Fix $s \in \{1,2,\dots,k\}$. For $v \in \{1,\dots,k-s+1\}$ we have $\mathrm{LM}(g_{s,v}) = x_s^{q^{s+v-1}-q^{s-1}}$. In particular, $\mathrm{LM}(g_s) = x_s^{q^k-q^{s-1}}$.*

Proof. We have $\sum_{i=0}^{s} d_{s,i}t^{q^i} = \prod_{(a_1,a_2,\dots,a_s)\in F^s}(t+a_1x_1+a_2x_2+\cdots+a_sx_s)$. Since x_s appears in $q^s - q^{s-1}$ terms in the above product, the leading monomial of $d_{s,s-1}$ is $x_s^{q^s-q^{s-1}}$. Similarly for $0 \leq j < s-1$ the degree of $d_{s,j}$ is greater than $q^s - q^{s-1}$ and so no monomial in $d_{s,j}$ is a power of x_s.

Note that the assertion of the lemma holds trivially for $v = 0$. Also for $s = 1$, we have $g_{1,v} = -d_{1,0}^{q^{v-1}}\, g_{1,v-1}$; hence the assertion again follows easily by induction on v. More generally, we write

$$g_{s,v} = -\big(d_{s,s-1}^{q^{v-1}}\, g_{s,v-1} + \cdots\big).$$

Note that

$$\begin{aligned} \mathrm{LM}(d_{s,s-1}^{q^{v-1}}\, g_{s,v-1}) &= \mathrm{LM}(d_{s,s-1}^{q^{v-1}})\, \mathrm{LM}(g_{s,v-1}) = x_s^{(q^s-q^{s-1})(q^{v-1})} x_s^{q^{s+v-2}-q^{s-1}} \\ &= x_s^{q^{s+v-1}-q^{s-1}} \end{aligned}$$

because $\mathrm{LM}(g_{s,v-1}) = x_s^{q^{s+v-2}-q^{s-1}}$ by induction. Since no monomial in $d_{s,j}$ is a power of x_s for $j < s-1$, and $g_{s,v} + d_{s,s-1}^{q^{v-1}}\, g_{s,v-1}$ lies in the ideal in $F[x_1, x_2, \dots, x_s]$ generated by $d_{s,0}, d_{s,1}, \dots, d_{s,s-2}$, it follows that $\mathrm{LM}(g_{s,v}) = \mathrm{LM}(d_{s,s-1}^{q^{v-1}}\, g_{s,v-1})$, which completes the proof. □

We now prove a relation.

Lemma 2. *For any s in $\{1, 2, \dots, k\}$,*

$$\sum_{v=0}^{k-s+1} d_{k,s+v-1}\, g_{s,v} = 0.$$

Proof. For s in $\{1, 2, \dots, k\}$ we consider

$$\begin{aligned}
f_k(t) &= \prod_{(a_1,a_2,\dots,a_k)\in F^{\times k}} (t + a_1x_1 + a_2x_2 + \cdots + a_kx_k) \\
&= \prod_{(a_{s+1},a_{s+2}\dots,a_k)\in F^{\times (k-s)}} f_s(t + a_{s+1}x_{s+1} + \cdots + a_kx_k) \\
&= \prod_{(a_{s+1},a_{s+2}\dots,a_k)\in F^{\times (k-s)}} (f_s(t) + a_{s+1}f_s(x_{s+1}) + \cdots + a_kf_s(x_k)) \\
&= f_{f_s(x_{s+1}),\dots,f_s(x_k)}(f_s(t)) \\
&= \sum_{i=0}^{k-s} \big(d_{k-s,i}(f_s(x_{s+1}), \dots, f_s(x_k)) \sum_{j=0}^{s} (d_{s,j}^{q^i} t^{q^{i+j}})\big).
\end{aligned}$$

Denote $d_{k-s,i}(f_s(x_{s+1}), \dots, f_s(x_k))$ by $A_{s,i}$. Considering the coefficients of t^{q^v} on both sides of the above equation we get

$$d_{k,v} = \sum_{\substack{i+j=v\\ 0\le i\le k-s\\ 0\le j\le s}} A_{s,i}\, d_{s,j}^{q^i} = \sum_{i\,=\,\max\{0,v-s\}}^{\min\{k-s,v\}} A_{s,i}\, d_{s,v-i}^{q^i}.$$

Therefore

$$\begin{aligned}
\sum_{v=0}^{k-s+1} d_{k,s+v-1}\, g_{s,v} &= \sum_{v=0}^{k-s+1} \left(\sum_{i=\max\{0,v-1\}}^{\min\{k-s,s+v-1\}} A_{s,i}\, d_{s,s+v-1-i}^{q^i} \right) g_{s,v} \\
&= \sum_{i=0}^{k-s} \sum_{v=\max\{0,i-s+1\}}^{i+1} A_{s,i}\, d_{s,s+v-1-i}^{q^i}\, g_{s,v} \\
&= \sum_{i=0}^{k-s} A_{s,i} \sum_{v=\max\{0,i-s+1\}}^{i+1} d_{s,s+v-1-i}^{q^i}\, g_{s,v} \\
&= \sum_{i=0}^{k-s} A_{s,i} \left(g_{s,i+1} + \sum_{v=0}^{\min\{i,s-1\}} d_{s,s-v-1}^{q^i}\, g_{s,i-v} \right) = 0,
\end{aligned}$$

as desired. □

We are now ready to state our main result.

Theorem 3. *The set $\{g_1, g_2, \ldots, g_k\}$ is the reduced Gröbner basis for the Hilbert ideal $R^G_+ \cdot R$.*

Proof. By Lemma 1, the leading monomials of g_i for $1 \leq i \leq k$ are relatively prime and no monomial in g_i is divisible by a leading monomial of g_j for $i \neq j$. Therefore it is enough to show that the ideal I generated by $\{g_1, g_2, \ldots, g_k\}$ is equal to $R^G_+ \cdot R$.

Observe that the assertion of Lemma 2 is equivalent to

$$d_{k,s-1} + \sum_{v=1}^{k-s} d_{k,s+v-1}\, g_{s,v} = g_s$$

for any s in $\{1, 2, \ldots, k\}$. So it follows that $I \subseteq R^G_+ \cdot R$. Conversely notice that $d_{k,k-1} = g_k$. Furthermore, assuming that $d_{k,k-1}, d_{k,k-2}, \ldots, d_{k,j} \in I$ one gets $d_{k,j-1} \in I$ by putting $s = j$ in the above equation. This shows by induction that $d_{k,k-1}, d_{k,k-2}, \ldots, d_{k,0} \in I$. Hence $R^G_+ \cdot R \subseteq I$. □

In the context of Equation 1, define $m = \min(s, v)$. By an ordered (s, v)-partition we mean a sequence of positive integers $i_1, i_2, \ldots, i_n$ with $n \in \mathbb{Z}_{\geq 0}$, $i_1 + i_2 + \cdots + i_n = v$ and $1 \leq i_j \leq m$. We let $P_{s,v}$ denote the set of all (s, v)-partitions. For $p = i_1, i_2, \ldots, i_n \in P_{s,v}$, define

$$f_p = \prod_{1 \leq j \leq n} d^{q^{e_j}}_{s,s-i_j},$$

where $e_1 = v - 1$ and $e_j = v - 1 - \sum_{k=1}^{j-1} i_k$ for $n \geq j \geq 2$. Furthermore, $d(p) := n$ is called the length of p. We describe $g_{s,v}$ in terms of Dickson invariants of dimension s in the next proposition. Recall that the s-th Gröbner basis element g_s is equal to $-g_{s,k-s+1}$.

Proposition 4. *For $s \in \{1, 2, \ldots, k\}$ and $v \in \{1, 2, \ldots, k - s + 1\}$ we have*

$$g_{s,v} = \sum_{p \in P_{s,v}} (-1)^{d(p)} f_p.$$

Proof. We fix s and proceed by induction on v. For $v = 1$, we have only one element in $P_{s,1}$, which is the partition $1 = 1$ whose length is one, and therefore $\sum_{p \in P_{s,1}} (-1)^{d(p)} f_p = -d_{s,s-1}$ as required. Note that Equation 1 is equivalent to

$$g_{s,v} = -\big(\sum_{j=1}^{m} d^{q^{v-1}}_{s,s-j}\, g_{s,v-j}\big).$$

Then $g_{s,v-j} = \sum_{p \in P_{s,v-j}} (-1)^{d(p)} f_p$ for $1 \leq j \leq m$ by induction. For $p = i_1, i_2, \ldots, i_n \in P_{s,v-j}$ we have

$$-d^{q^{v-1}}_{s,s-j} (-1)^{d(p)} f_p = -(-1)^{d(p)} d^{q^{v-1}}_{s,s-j} \prod_{1 \leq j \leq n} d^{q^{e_j}}_{s,s-i_j} = (-1)^{d(p')} f_{p'},$$

where $p' = j, i_1, i_2, \ldots, i_n \in P_{s,v}$. It follows that the terms in the summation $-(\sum_{j=1}^{m} d^{q^{v-1}}_{s,s-j}\, g_{s,v-j})$ are all in the form $(-1)^{d(p')} f_{p'}$ for some $p' \in P_{s,v}$. Conversely every ordered partition $p' = j, i_1, i_2, \ldots, i_n$ in $P_{s,v}$ can be obtained by adding j as the first element to the ordered partition $i_1, i_2, \ldots, i_n$ in $P_{s,v-j}$. Furthermore, this process is injective. It follows that for each $p' \in P_{s,v}$, the term $(-1)^{d(p')} f_{p'}$ appears exactly once in the summation $-(\sum_{j=1}^{m} d^{q^{v-1}}_{s,s-j}\, g_{s,v-j})$. This completes the proof. □

References

1. H. E. A. Campbell, I. P. Hughes, R. J. Shank, and D. L. Wehlau, *Bases for rings of coinvariants*, Transform. Groups **1** (1996), no. 4, 307–336. MR1424447 (98a:13011)
2. Leonard Eugene 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), no. 1, 75–98. MR1500882
3. Robert Steinberg, *On Dickson's theorem on invariants*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **34** (1987), no. 3, 699–707. MR927606 (89c:11177)
4. Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996. MR1363949 (97b:13034)
5. Clarence Wilkerson, *A primer on the Dickson invariants*, Proceedings of the Northwestern Homotopy Theory Conference (Evanston, Ill., 1982), Contemp. Math., vol. 19, Amer. Math. Soc., Providence, RI, 1983, pp. 421–434. MR711066 (85c:55017)

Department of Mathematics, Bilkent University, Ankara 06800, Turkey

Department of Mathematics, Bilkent University, Ankara 06800, Turkey