An Algorithm to Determine Properties of Field Extensions Lying over a Ground Field*

Gregor Kemper†

October 10, 1993

Let $K \leq L \leq N$ be fields such that N is finitely generated over K. We will use Gröbner basis methods to calculate the transcendence degree of $N|L$ and the degree $[N:L]$ if the extension is algebraic. There is another, similar proof for most of the results of this paper in [Sw1]. See also the closely related work [S-S] and the report [Sw2]. What is new here is a somewhat more structural understanding of the extension $N|L$, gained by looking at a chain of subfields between L and N, and a stronger result on the minimal polynomials that the algorithm will produce (see Proposition 2 (c)).

The main purpose of the paper, though, is to lay the theoretical grounds for an implementation of the algorithm which was done by the author using the *Maple* computer language ([Ma]). Section 2 is devoted to the description of it. We will also take a look at some examples of application. The second of these, verifying solutions of *Noether's Problem*, was the main motivation for me to implement the algorithm.

*This article also appeared as IWR-Preprint **93-58**.

†The author is supported by the Graduiertenkolleg "Modellierung und wissenschaftliches Rechnen in Mathematik und Naturwissenschaften" which is funded by the DFG and the Land Baden-Württemberg.

Contents

1 The Theory

Let us fix some notation first.

$L|K$ is finitely generated, too, as will be shown in the Appendix. Say $N = K(\vartheta_1, \ldots, \vartheta_n)$ and $L = K(\varphi_1, \ldots, \varphi_m)$, then

$$\varphi_i = g_i(\vartheta_1, \ldots, \vartheta_n) \text{ with } g_i \in K(X_1, \ldots, X_n),$$

the field of rational functions in n indeterminates. By Hilbert's Basissatz, the kernel of

$$K[X_1, \ldots, X_n] \to N,\ X_i \mapsto \vartheta_i.$$

is a finitely generated ideal in $K[X_1, \ldots, X_n]$. Let $r_1, \ldots, r_s$ be generators for it.

The basic idea is very simple: Take the equations

$$r_i = 0\ (i = 1, \ldots, s) \text{ and } T_i = g_i\ (i = 1, \ldots, m)$$

with additional indeterminates T_i, and try to solve these equations for the X_i. This crude idea still requires some refinement and elaboration, though.

In the sequel we will use the abbreviations $\underline{X}$ for $X_1, \ldots, X_n$, $\underline{g}$ for $g_1, \ldots, g_m$ and so on. If G is a Gröbner basis, then by a G-residue of some polynomial f we mean the result of successively eliminating the lead term of f and of its descendants by adding a multiple of an element of G whose lead monomial divides the lead monomial of f (or its descendant). In particular, all members of the ideal generated by G have the G-residue zero.

1.1 A Special Case

First we prove two propositions for a special case and then the main result (Theorem 1), which itself turns out to be essentially a special case of Proposition 2.

Proposition 1 *Suppose that in the above situation all g_i lie in $K[\underline{X}]$. Let $T_1, \ldots, T_m$ be additional indeterminates and*

$$I = (r_1, \ldots, r_s, T_1 - g_1, \ldots, T_m - g_m) \trianglelefteq K[\underline{T}, \underline{X}].$$

Then I is the kernel of the K-algebra homomorphism

$$K[\underline{T}, \underline{X}] \to N,\ T_i \mapsto \varphi_i,\ X_i \mapsto \vartheta_i.$$

Proof. It is clear that I lies in the kernel.

Let $P(\underline{T})$ be a product of T_i's. We show by induction over the degree ∂P of P that

$$P(\underline{T}) - P(\underline{g}) \in I.$$

There is nothing to show for $\partial P = 0$.

Let $\partial P > 0$, then $P(\underline{T}) = T_i \cdot P'(\underline{T})$ where $\partial P' < \partial P$. By induction we have $P'(\underline{T}) - P'(\underline{g}) \in I$, and we conclude

$$P(\underline{T}) - P(\underline{g}) = (T_i - g_i) \cdot P'(\underline{T}) + g_i \cdot \left(P'(\underline{T}) - P'(\underline{g})\right) \in I.$$

Having shown this, it follows that for all $f(\underline{T}, \underline{X}) \in K[\underline{T}, \underline{X}]$ we have

$$f(\underline{T}, \underline{X}) - f(\underline{g}, \underline{X}) \in I.$$

But if f lies in the kernel, then $f(\underline{g}, \underline{X}) \in (r_1, \ldots, r_s)$ and hence $f(\underline{T}, \underline{X}) \in I$. ■

Proposition 2 *Again suppose that all $g_i \in K[\underline{X}]$, and let T_i and I be as in Proposition 1. Let $\pi \in S_n$ be any permutation of the indices $1, \ldots, n$. Using a term order $\prec$ on $K[\underline{T}, \underline{X}]$ with the property*

$$X_{\pi(i)} \succ \left(\textit{any monomial in } T_1, \ldots, T_m, X_{\pi(1)}, \ldots, X_{\pi(i-1)}\right),$$

let G be a minimal Gröbner basis of I. (By "minimal" we mean that the lead monomial of any member of G does not divide the lead monomial of any other.) Set

$$G_T = G \cap K[\underline{T}],\ G_i = G \cap K[\underline{T}, X_{\pi(1)}, \ldots, X_{\pi(i)}] \setminus K[\underline{T}, X_{\pi(1)}, \ldots, X_{\pi(i-1)}]$$

and

$$L_i = L(\vartheta_{\pi(1)}, \ldots, \vartheta_{\pi(i)}) \leq N.$$

Then the following holds

(a) G_T generates the kernel of $K[\underline{T}] \to L,\ T_i \mapsto \varphi_i$.

(b) The transcendence degree of $N|L$ is equal to the number of G_i's which are empty.

(c) If all G_i's are non-empty, let f_i be a minimal member of G_i with respect to the term order $\prec$, and let $e_i = \partial_{\pi(i)}(f_i)$ be the $X_{\pi(i)}$-degree of f_i. Then the lead monomial of f_i contains no $X_{\pi(j)}$ with $j \neq i$, and substituting $T_j = \varphi_j$ for all j and $X_{\pi(j)} = \vartheta_{\pi(j)}$ for $j < i$ in f_i yields a minimal polynomial for $\vartheta_{\pi(i)}$ over L_{i-1} (which need not be monic). In particular, we have the formula

$$[N : L] = \prod_{i=1}^{n} e_i.$$

Proof. G_T lies in $I \cap K[\underline{T}]$ and hence in the kernel.

Conversely, take $f(\underline{T}) \in K[\underline{T}]$ such that $f(\underline{\varphi}) = 0$. Then $f \in I$ by Proposition 1, so f has the G-residue 0. Since $X_i \succ K[\underline{T}]$ for all i, f must even have the G_T-residue 0. Hence $f \in (G_T)$, which completes the proof of (a).

To show (b) and (c) we consider the extension $L_i|L_{i-1}$ for a fixed i.

If $G_i \neq \emptyset$, let $f(\underline{T}, X_{\pi(1)}, \ldots, X_{\pi(i)}) \in G_i$ and set $\bar{f}(X_{\pi(i)}) = f(\underline{\varphi}, \vartheta_{\pi(1)}, \ldots, \vartheta_{\pi(i-1)}, X_{\pi(i)}) \in L_{i-1}[X_{\pi(i)}]$. Assuming that $\partial \bar{f} < \partial_{\pi(i)}(f)$, we conclude that f as a polynomial in $X_{\pi(i)}$ has a highest coefficient c which lies in $I \cap K[\underline{T}, X_{\pi(1)}, \ldots, X_{\pi(i-1)}]$. Then the leading monomial $\mathrm{LM}(c)$ of c is divisible by the leading monomial of some $f' \in G_j$ with $j < i$; but by the property of the term order $\mathrm{LM}(c)$ divides the leading monomial of f, contradicting the minimality of G.

Thus we have $\partial \bar{f} = \partial_{\pi(i)}(f) > 0$. But $\bar{f}(\vartheta_{\pi(i)}) = 0$, so L_i is algebraic over L_{i-1}.

On the other hand, let $L_i | L_{i-1}$ be algebraic and let $0 \neq \bar{f}(X_{\pi(i)}) \in L_{i-1}[X_{\pi(i)}]$ such that $\bar{f}(\vartheta_{\pi(i)}) = 0$. By multiplying $\bar{f}$ by a constant from L_{i-1} we may assume that $\bar{f}(X_{\pi(i)}) \in K[\underline{\varphi}, \vartheta_{\pi(1)}, \ldots, \vartheta_{\pi(i-1)}]\left[X_{\pi(i)}\right]$ without changing its degree. Let $f \in K[\underline{T}, X_{\pi(1)}, \ldots, X_{\pi(i-1)}, X_{\pi(i)}]$ such that substituting $T_j = \varphi_j$ and $X_{\pi(j)} = \vartheta_{\pi(j)}$ $(j < i)$ in f yields $\bar{f}$. Then $f \in I$ by Proposition 1, so f must have the G-residue 0. We may assume that f is already reduced by all members of G_j, $j < i$. Then the lead monomial of f must be divisible by the lead monomial of some member of G_i. In particular, $G_i \neq \emptyset$.

We have shown that the transcendence degree of L_i / L_{i-1} is 0 iff $G_i \neq \emptyset$ and 1 otherwise. Part (b) of the Proposition now follows immediately.

To prove (c), let all G_i's be non-empty. Then $N | L$ is algebraic and thus $L_i = L[\vartheta_{\pi(1)}, \ldots, \vartheta_{\pi(i)}]$ for all i. Fix any i. There exists $\bar{f}(X_{\pi(i)}) \in K[\underline{\varphi}, \vartheta_{\pi(1)}, \ldots, \vartheta_{\pi(i-1)}]\left[X_{\pi(i)}\right]$ with $\bar{f}(\vartheta_{\pi(i)}) = 0$, such that the highest coefficient of $\bar{f}$ contains no ϑ_j and $\partial \bar{f} = [L_i : L_{i-1}]$. By the above there must exist an $h \in G_i$ with $\partial_{\pi(i)}(h) = [L_i : L_{i-1}]$, whose lead monomial contains no $X_{\pi(j)}$ with $j \neq i$.

Let h' be a minimal element of G_i with respect to the term order. We have seen that specializing $T_j = \varphi_j$ and $X_{\pi(j)} = \vartheta_{\pi(j)}$ $(j < i)$ in h' yields a polynomial $\overline{h'}(X_{\pi(i)})$ with $\partial \overline{h'} = \partial_{\pi(i)}(h')$ and $\overline{h'}(\vartheta_{\pi(i)}) = 0$, so $\partial_{\pi(i)}(h') \geq [L_i : L_{i-1}]$. The minimality of h' now yields $\partial_{\pi(i)}(h') = \partial_{\pi(i)}(h)$, so $\overline{h'}(X_{\pi(i)})$ is a minimal polynomial for $\vartheta_{\pi(i)}$ over L_{i-1}. By the minimality of h' we also get that the lead monomial of h' contains no $X_{\pi(j)}$ with $j \neq i$.

This completes the proof of (c). ■

1.2 The General Case

We can turn to the general case now. The idea is to use the equations

$$(\text{numerator of } g_i) - T_i \cdot (\text{denominator of } g_i)$$

instead of $T_i - g_i$, and to include equations that will rule out solutions for which some of the denominators are zero.

Theorem 1 *Using the notation introduced above, let* $g_i = \frac{n_i}{d_i}$ *with* n_i, $d_i \in K[\underline{X}]$ *and take* $p_1, \ldots, p_k \in K[\underline{X}] \setminus (r_1, \ldots, r_s)$ *such that for the product* $d = p_1 \cdots p_k$ *there exists a natural number* e *with* $d_i \mid d^e$ *for all* i. *(In the implementation, the* p_i*'s will be those prime polynomials which occur as divisors of some* d_i*.) Introduce new indeterminates* $U_1, \ldots, U_k$ *and* $T_1, \ldots, T_m$ *and set*

$$\begin{aligned} I &= \big(p_1 \cdot U_1 - 1, \ldots, p_k \cdot U_k - 1,\, r_1, \ldots, r_s, \\ &\qquad n_1 - T_1 \cdot d_1, \ldots, n_m - T_m \cdot d_m\big) \trianglelefteq K[\underline{T}, \underline{X}, \underline{U}]. \end{aligned}$$

Let $\pi \in S_n$ *be any permutation of the indices* $1, \ldots, n$. *Using a term order* $\prec$ *on* $K[\underline{T}, \underline{X}, \underline{U}]$ *with the properties*

$$U_i \succ \big(\textit{any monomial in } \underline{T} \textit{ and } \underline{X}\big) \textit{ and}$$

$$X_{\pi(i)} \succ \big(\textit{any monomial in } \underline{T},\, X_{\pi(1)}, \ldots, X_{\pi(i-1)}\big),$$

let G *be a minimal Gröbner basis of* I.

Define G_T, G_i *and* L_i *as in Proposition 2, then the statements (a)-(c) from Proposition 2 hold.*

Proof. Set $\delta_i = 1/p_i(\vartheta_1, \ldots, \vartheta_n)$. It is verified by some calculation that the kernel of

$$K[\underline{X}, \underline{U}] \to N,\ X_i \mapsto \vartheta_i,\ U_i \mapsto \delta_i$$

is exactly the ideal spanned by $p_i \cdot U_i - 1$ $(i = 1, \ldots, k)$ and r_i $(i = 1, \ldots, s)$. The key observation is that

$$(p_i U_i)^i - 1 = (p_i U_i - 1) \cdot \sum_{\nu=0}^{i-1} (p_i U_i)^\nu \in \big(p_i U_i - 1\big). \tag{1}$$

Now set $g_i' = (d \cdot U_1 \cdots U_k)^e\, g_i \in K[\underline{X}, \underline{U}]$ and

$$I' = (p_1 U_1 - 1, \ldots, p_k U_k - 1,\, r_1, \ldots, r_s,\, T_1 - g_1', \ldots, T_m - g_m').$$

Then clearly $g_i'(\underline{\vartheta}, \underline{\delta}) = g(\underline{\vartheta}, \underline{\delta})$, and another calculation shows that $I' = I$.

Since I includes linear equations for the U_i, G will also be a Gröbner basis with respect to a term order which satisfies the slightly stronger condition

$$U_{\tau(i)} \succ \Big(\text{any monomial in } \underline{\mathrm{T}},\ \underline{\mathrm{X}} \text{ and } U_{\tau(1)}, \ldots, U_{\tau(i-1)}\Big)$$

for some permutation τ of the indices $1, \ldots, k$.

These observations show that we are exactly in the situation of Proposition 2, so Theorem 1 is actually a special case of Proposition 2. ■

2 The Implementation

The algorithm stated in Theorem 1 has been implemented as a *Maple* procedure called "`extension`". This procedure is the main part of the program package "*fields*" which as another major procedure contains "`normalform`" (see below). As there is on-line help for the syntactical aspects of the package, we will only make a few notes here and give some examples of usage, keeping the notation from the introduction and Theorem 1.

2.1 Some Remarks

- The ground field K can be either $\mathbb{Q}$ or an algebraic number field. In the latter case, K is defined by the minimal polynomial of a generating algebraic number α, and elements of K are represented as polynomials in α with rational coefficients.

- Theorem 1 leaves a large variety of choices for the p_i's. Experience seems to indicate that the highest speed is obtained by taking all prime polynomials which occur as divisors of some d_i, although this choice has the disadvantage of producing many additional variables U_i to calculate with. (But this seems to weigh little since there are linear equations for the U_i.) This would be an answer to a question posed by M. Sweedler in [Sw1]. Another obvious choice would be to take only one p_i, namely the square-free part of the common denominator of the g_i's. There is an option in `extension` which lets the user specify his own p_i's.

- N is given by its relations $r_1, \ldots, r_s$, and L is given by the g_i's. So the question arises what will happen if one of the denominators of the g_i evaluates to zero modulo $\mathfrak{r} = (r_1, \ldots, r_s)$, or if $\mathfrak{r}$ is not a prime ideal or (even worse) equals (1). All these cases can be subsumed by the condition (C) that some power of the product of denominators of the g_i lies in $\mathfrak{r}$. Since $(U_1 \cdots U_k \cdot d)^e \equiv 1 \pmod{I}$ by Formula (1) in the proof of Theorem 1, (C) is equivalent to the condition $I = (1)$. So the occurrence of (C) is easily diagnosed by `extension`. If, on the other hand, condition (C) does not hold, then the results computed by `extension` still make sense even if $\mathfrak{r}$ is not a prime ideal by considering $K[\underline{\vartheta}, \frac{1}{d(\underline{\vartheta})}]$ instead of N.

- The permutation π of the X_i is chosen by a *Maple* library routine which reorders variables from a list of polynomials to make them "heuristically optimal" for Gröbner basis computations.

- G_T is a Gröbner basis for the kernel of $K[\underline{T}] \to L$, $T_i \mapsto \varphi_i$, and since the implementation uses a lexicographic term order on the T_i's, the transcendence degree of $L|K$ equals the number of T_i's which do not occur in G_T by an argument analogous to that given in the proof of Proposition 2. The transcendence degree of $L|K$ is returned by `extension` as one of its results.

- The really hard part of the algorithm is the computation of a Gröbner basis for I. But specializing some of the T_i's for which the corresponding φ_i's are assumed to be algebraically independent to random values will yield good probabilistic results for the transcendence degrees and for $[N{:}L]$, if finite. On the other hand, this will make the computation much quicker. This option is supported by `extension`.

  In my experience I never got a wrong result from specializing!

- The routine `normalform` calculates normal forms of elements of N in the following sense: After `extension` has been called, we have minimal polynomials for each $\vartheta_{\pi(i)}$ over L_{i-1} where $L_i|L_{i-1}$ is algebraic. Then every element of L_i has a normal form as a polynomial in $\vartheta_{\pi(i)}$ of degree less than $[L_i{:}L_{i-1}]$. Or if $L_i|L_{i-1}$ is not algebraic, then the normal form is a rational function in $\vartheta_{\pi(i)}$ with coefficients in L_{i-1}. Descending along

the chain

$$N = L_n \geq L_{n-1} \geq \ldots \geq L_1 \geq L_0 = L$$

yields a normal form for an element of N. The routine `normalform` calculates this normal form for elements of $K[\underline{\vartheta}]$. For fractions, the quotient of the normal form of the numerator over that of the denominator is returned. In particular, this provides a membership test for L.

2.2 Installation

The *fields* package runs with *Maple V* and beyond. The package can be obtained directly from the author (The email address is at the end of this paper) or from the electronic share library of *Maple*, which can be accessed via anonymous ftp. The sites are

Internet address	Symbolic address	Site location
129.132.101.33	neptune.inf.ethz.ch	Zurich, Switzerland
129.97.140.58	daisy.waterloo.edu	Waterloo, Canada

What you need to get is the main file `fields` and maybe the test file `fields.test`. Suppose you have them sitting in the current working directory. Then you call *Maple* and do the following:

```
> read fields;
> # The procedures are now defined and saved in  fields.m.
> # If using MapleV Rel. 1, you have to say   _liblist:=[`.`]:
> with(fields):
> ?fields
```

Now you should get on-line help for the package, and you can start using it. If you type

```
> read `fields.test`;
```

you should get a series of `okay`'s.

2.3 Examples

We now give two examples of the *fields* package at work. The following listings are taken from *Maple* sessions using the version *Maple V Release 2*.

The first example is motivated by the idea of spherical coordinates. We take $K = \mathbb{Q}\left(\sqrt{-1}\right)$ as ground field ($\mathbb{Q}$ would work, too). N is the field of rational functions in x, y and z, and we generate L by the three functions

$$r = x^2 + y^2 + z^2,\ \varphi = \frac{y}{x} \text{ and } \vartheta = \frac{z^2}{x^2 + y^2},$$

which are "almost" spherical coordinates.

```
> interface(screenwidth=63); gc(0):
> read fields;
> with(fields):
> minpol:=a^2+1:                                  # define K
> gens:={r=x^2+y^2+z^2,f=y/x,t=z^2/(x^2+y^2)}:
>
> # The global variable  protocol_level  controls how much
> # information  extension  will print out during execution
> protocol_level:=2:
>
> # Put the minimal polynomials into 'basis'. The ground field
> # K is communicated to  extension  be the equation for mipo.

> extension(gens,mipo=minpol,'basis');
Given Situation:

                          K=Q(a) with

                           2
                          a  + 1 = 0,


                          N=K(x,y,z),
```

L=K(r,t,f) with

$$r = x^2 + y^2 + z^2,\ f = y/x,\ t = \frac{z^2}{x^2 + y^2}$$

Calculating the prime divisors of the denominators of the g_i
... done
They are:

[x, x + a y, x - a y]

Take the term order with u[2] > u[3] > u[1] > z > y > x > r > t > f

Calculating a Groebner basis of I ...
... done

Results:

N|L is algebraic of degree 4

Minimal polynomials:

z: $z^2 + f^2 x^2 + x^2 - r$

y: $y - f x$

x: $(1 + f^2 + t + t f^2) x^2 - r$

L|K has transcendence degree 3

```
Time used: 6.383 sec
                                4

> # The degree [N:L] is returned by  extension.
>
> # Interpretation: For every (sufficiently general) choice of
> # r,f and t there are four points having these "coordinates".
> # This agrees with what one would intuitively expect!
>
> # Does y^2 lie in L?
> normalform(y^2,basis);

                              2
                             f  r
                    -----------------
                         2          2
                    1 + f  + t + t f

> # It does! Check this ...
> normal(subs(gens,"));

                               2
                              y
> # All right!
```

In the next example we verify a solution of *Noether's Problem* for the group A_4, i.e. we show that the field of invariants under A_4 acting on the field $\mathbb{Q}(x_1, \ldots, x_4)$ of rational functions by permuting the indeterminates can be generated by (no more than) four invariants. A generating set of five elements is given by the elementary symmetric polynomials $s_1, \ldots, s_4$ and the expression

$$d = \prod_{i<j} (x_i - x_j),$$

where d satisfies the discriminant relation

$$d^2 = \mathrm{Discr}\left(x^4 - s_1 x^3 + s_2 x^2 - s_3 x + s_4\right).$$

To make the computation simpler, we change s_2, s_3 and s_4 by substituting $x_i \to x_i - s_1/4$. Then d satisfies the above discriminant relation, but *without* the x^3-term. This means that s_1 is algebraically independent over $N = \mathbb{Q}(\sim_{\not\vdash}, \sim_{\not\vdash}, \sim_{\not\vdash},)$, so now we have to generate N by *three* invariants. The theory (that I don't want to go into here) yields candidates for such generating invariants, which are

$$\varphi_1 = \frac{s_3}{s_2},\ \varphi_2 = \frac{12s_2s_4 + s_2^3}{d},\ \varphi_3 = \frac{27s_3^2 + 8s_2^3}{d}.$$

But it is still not certain whether these invariants actually generate all of N. So here is a listing of the *Maple* session where it is verified that $N = \mathbb{Q}(\varphi_{\not\vdash}, \varphi_{\not\vdash}, \varphi_{\not\vdash})$.

```
> interface(screenwidth=63); gc(0):
> read fields;
> with(fields):
> rel:=d^2-discrim(x^4+s2*x^2-s3*x+s4,x);

           2       3   2        4           4         2   2
    rel := d  + 4 s2  s3  + 27 s3  - 16 s4 s2  + 128 s4  s2

                    2           3
         - 144 s2 s3  s4 - 256 s4

> gens:={g1=s3/s2,g2=(12*s2*s4+s2^3)/d,g3=(27*s3^2+8*s2^3)/d};

                                      3            2       3
               s3        12 s2 s4 + s2        27 s3  + 8 s2
 gens := {g1 = ----, g2 = --------------, g3 = --------------}
               s2               d                    d

> # The equation indep=all tells  extension  that all g_i's are
> # assumed algebraically independent. This speeds up the
> # calculation. The relation is given by the equation for r.
>
> extension(gens,r=rel,indep=all);
Calculating the prime divisors of the denominators of the g_i
```

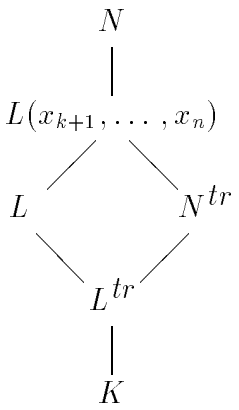
```
... done
Calculating a Groebner basis of I ...
... done

Results:

L=N

L|K has transcendence degree 3

                                1

> # So actually L=N, and Noether's Problem is solved!
> time();
                              8.766
```

Appendix

As promised in the introduction, we will now show that L is finitely generated over K.

Proposition 0 *Let $K \leq L \leq N$ be fields such that N is finitely generated over K. Then so is L.*

Proof. $L|K$ is of finite transcendence degree. Let $x_1, \ldots, x_k$ be a transcendence basis. It can be extended to a transcendence basis $x_1, \ldots, x_n$ of $N|K$. Set $L^{tr} = K(x_1, \ldots, x_k)$ and $N^{tr} = K(x_1, \ldots, x_n)$. We have the following diagram



Since N is finite over N^{tr} by the assumption, so is $L(x_{k+1}, \ldots, x_n)$.

Let $b_1, \ldots, b_s \in L$ with $s > \left[L(x_{k+1}, \ldots, x_n) : N^{tr}\right]$. Then they are linearly dependent over N^{tr}, say

$$\sum_{i=1}^{s} \alpha_i b_i = 0 \text{ with } \alpha_i \in N^{tr} = L^{tr}(x_{k+1}, \ldots, x_n),$$

not all zero. We may assume $\alpha_i \in L^{tr}[x_{k+1}, \ldots, x_n]$. The equation lives in $L[x_{k+1}, \ldots, x_n]$, and since $x_{k+1}, \ldots, x_n$ are algebraically independent over L, it must hold coefficient-wise. But some coefficient of some α_i is non-zero, and we get a non-trivial linear equation for the b_i over L^{tr}.

Hence L is finite over L^{tr}, which completes the proof. ■

References

[Ma] B. Char, K. Geddes, G. Gonnet, M. Monagan and S. Watt, *Maple Reference Manual (5th Edn.)*, Waterloo Maple Publishing, Waterloo, Ontario, 1990

[S-S] David Shannon and Moss Sweedler, *Using Gröbner Bases to Determine Algebra Membership, Split Surjective Algebra Homomorphisms, and to Determine Birational Equivalence*, J. of Symbolic Computation **6** (1988), 267–273

[Sw1] M.Sweedler, *Using Gröbner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: Return of the Killer*

Tag Variables, in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (Gérard Cohen, Teo Mora, Oscar Moreno Eds.), Springer LNCS **673** (1993), 66–75

[Sw2] Moss Sweedler, *Using Gröbner Bases to Determine the Nature of Field Extensions*, Transactions of the Ninth Army Conference on Applied Mathematics and Computing, ARO Report 92-1, 1992

Gregor Kemper
IWR
Im Neuenheimer Feld 368
69 120 Heidelberg
Germany

email `kemper@kalliope.iwr.uni-heidelberg.de`