MATH. SCAND. 6 (1958), 40–46

THE DETERMINATION OF FIELDS OF SMALL DISCRIMINANT WITH A GIVEN SUBFIELD

H. J. GODWIN

1. In some recent papers [1] [2] [3] I have developed a method for the determination of all the fields which are of given degree and signature, have no subfield, and have discriminants bounded by some chosen value. In the present paper[1] I extend this method to the case of fields having a given subfield other than the rational field, but before coming to this case it may be helpful to remind the reader of the method used in the simpler cases.

The integers of an algebraic field K of degree n can be represented as points of a lattice $\mathscr{L}_1$ in n dimensions: if complex numbers arise they do so in conjugate pairs and by using their real and imaginary parts we can ensure that $\mathscr{L}_1$ is real. The rational integers are represented by a line of points in $\mathscr{L}_1$ and by projecting on a space orthogonal to this line we obtain a lattice $\mathscr{L}_2$ in $n-1$ dimensions every point of which, except the origin, represents an integer of K. The determinant of $\mathscr{L}_2$ is a simple function of the discriminant Δ of K. For a given value of Δ we know that an ellipsoid, centered at the origin, with a given shape and a volume depending on Δ, will contain a point of $\mathscr{L}_2$: from this it follows that K (or a subfield other than the rational field) is generated by an algebraic number which is the zero of a polynomial, the zeros (and hence the coefficients) of which satisfy some inequality in terms of Δ. Not all polynomials so obtained lead to fields with discriminants within the bound with which we are working: it was suggested in [3] that by choosing the shape of the ellipsoid suitably we can minimize the number of unwanted polynomials which occur.

A subfield of K other than the rational field is represented by a sublattice of $\mathscr{L}_1$ of dimension greater than one: on projecting $\mathscr{L}_1$ on to the space orthogonal to this we obtain a lattice $\mathscr{L}_3$ and proceed with this as we did with $\mathscr{L}_2$ above. This is the essence of the proof of Theorem 1

Received July 20, 1957.

[1] I am grateful to a referee for a number of suggestions which led to improvements in the first draft of this paper.

below: this gives an inequality for the zeros of a polynomial defining K and involves the arbitrary positive numbers $l_1, \ldots, n_s$ which determine the shape of the ellipsoid used.

2. Notation. Let K be a field of degree $N = n\nu$ and discriminant Δ, possessing the subfield k of degree n, signature s and discriminant δ. K is generated by a zero θ of some polynomial

$$\Phi(x) = x^\nu + \lambda_1 x^{\nu-1} + \ldots + \lambda_\nu ,$$

the coefficients $\lambda_1, \ldots, \lambda_\nu$ of which are integers in k. On replacing $\lambda_1, \ldots, \lambda_\nu$ by their conjugates in k we obtain r real polynomials

$$\Phi_1(x), \ \ldots, \ \Phi_r(x)$$

and s pairs of complex conjugate polynomials

$$\Psi_1(x), \ \overline{\Psi}_1(x), \ \ldots, \ \Psi_s(x), \ \overline{\Psi}_s(x);$$

the zeros of all these are θ and its conjugates in K. Each $\Phi_j(x)$ will have an even number $2s_j$ of complex zeros, conjugate in pairs, but the zeros of the Ψ's must all be complex, since if α were a real zero of $\Psi_j(x)$ it would be a zero of $\overline{\Psi}_j(x)$ also, and so the conjugates of θ in K would not all be distinct.

Let the zeros of $\Phi_j(x)$ be

$$\alpha_{j,1}, \ \ldots, \ \alpha_{j,r_j}, \ \alpha_{j,r_j+1} \pm i\beta_{j,1}, \ \ldots, \ \alpha_{j,r_j+s_j} \pm i\beta_{j,s_j}$$

and of $\Psi_j(x)$ be

$$\gamma_{j,1} + i\varepsilon_{j,1}, \ \ldots, \ \gamma_{j,\nu} + i\varepsilon_{j,\nu}$$

where the α's, β's, γ's and ε's are all real.

3. We now state and prove the theorem referred to above.

Theorem 1. *There exists a polynomial $\Phi_1(x)$ such that*

$$\begin{aligned} 0 < \sum_{j=1}^{r} \left\{ \sum_{i=1}^{r_j+s_j} \alpha_{j,i}{}^2 - \Big(\sum_i \alpha_{j,i}\Big)^2 / (r_j + s_j) \right\} + \sum_{j=1}^{r} l_j{}^2 \left\{ \sum_{i=1}^{s_j} \beta_{j,i}{}^2 \right\} \\ + \sum_{j=1}^{s} m_j{}^2 \left\{ \sum_{i=1}^{\nu} \gamma_{j,i}{}^2 - \Big(\sum_i \gamma_{j,i}\Big)^2 / \nu \right\} + \sum_{j=1}^{s} n_j{}^2 \left\{ \sum_{i=1}^{\nu} \varepsilon_{j,i}{}^2 - \Big(\sum_i \varepsilon_{j,i}\Big)^2 / \nu \right\} \\ \leqq \gamma_{N-n} \left\{ \frac{|\Delta|^{\frac{1}{2}} \prod_{j=1}^{r} (\frac{1}{2} l_j)^{s_j} \prod_{j=1}^{s} (\frac{1}{2} m_j n_j)^{\nu-1}}{|\delta|^{\frac{1}{2}\nu^s} \prod_{j=1}^{r} (r_j + s_j)^{\frac{1}{2}}} \right\}^{\frac{2}{N-n}} \end{aligned}$$

where γ_{N-n} is Hermite's constant of order $N-n$ (that is, the critical determinant of an $N-n$ dimensional hypersphere of radius r is $r^{N-n}/\gamma_{N-n}^{\frac{1}{2}(N-n)}$). This polynomial $\Phi_1(x)$ either defines K as in section 2, or is a power of a polynomial $\chi_1(x)$ such that the zeros of $\chi_1(x)$ and its conjugates in k form a subfield of K.

Proof. The integers of K form a lattice $\mathscr{L}$ with determinant $\Delta^{\frac{1}{2}}$ which we transform into a real lattice $\mathscr{L}_1$ by operating on the pair of values α_j, $\gamma_{j+k} \pm i\beta_{j,k}$ with the matrix

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2}il_j & \frac{1}{2}il_j \end{pmatrix}$$

and on the pair of values $\gamma_{j,k} \pm i\varepsilon_{j,k}$ with the matrix

$$\begin{pmatrix} \frac{1}{2}m_j & \frac{1}{2}m_j \\ -\frac{1}{2}in_j & \frac{1}{2}in_j \end{pmatrix}$$

where $l_1, \ldots, n_s$ are arbitrary positive numbers; variation of these is equivalent to varying the shape of the ellipsoidal region in which we shall show the existence of lattice-points. The determinant of $\mathscr{L}_1$ is

$$\Delta^{\frac{1}{2}} \prod_j (\tfrac{1}{2}il_j)^{s_j} \prod_j (\tfrac{1}{2}im_j n_j)^v .$$

We then project $\mathscr{L}_1$ on to the $N-n$ dimensional space orthogonal to the space containing the integers of k, thus producing a lattice $\mathscr{L}_3$. The coordinates of a typical point of $\mathscr{L}_1$ may be taken to be

$$(\alpha_{1,1}, \ldots, \alpha_{1,r_1+s_1}, \alpha_{2,1}, \ldots, \alpha_{r,r_r+s_r}, m_1\gamma_{1,1}, \ldots, m_s\gamma_{s,v}, n_1\varepsilon_{1,1}, \ldots, n_s\varepsilon_{s,v}, l_1\beta_{1,1}, \ldots, l_r, \beta_{r,s_r})$$

and we carry out the projection by operating on $\mathscr{L}_1$ with the orthogonal matrix L constructed as follows. Let each of the submatrices

$$\mathsf{A}_1, \ldots, \mathsf{A}_r, \Gamma_1, \ldots, \Gamma_s, \mathsf{E}_1, \ldots, \mathsf{E}_s$$

be an orthogonal matrix with the elements in the first row all equal. A_j is of order r_j+s_j and the Γ's and E's are of order v. Then L is of order N and consists of $\mathsf{A}_1, \ldots, \mathsf{E}_s$ arranged diagonally, with the remaining places on the principal diagonal (equal in number to the number of β's) filled with 1's, and with zeros elsewhere. Let the set of rows of L containing first rows of $\mathsf{A}_1, \ldots, \mathsf{E}_s$ be denoted by R.

A point of $\mathscr{L}$ representing an integer of k is of the form

$$(a_1, \ldots, a_1, a_2, \ldots, a_r, c_1+ie_1, \ldots, c_s-ie_s)$$

each element occurring v times, and this becomes in $\mathscr{L}_1$ the point

$$(a_1, \ldots, a_1, a_2, \ldots, a_r, m_1c_1, \ldots, m_sc_s, n_1e_1, \ldots, n_se_s, 0, \ldots, 0) .$$

When L operates on this set of coordinates all rows other than those in R give zeros and so in general give the lattice $\mathscr{L}_3$. The first row of A_1 is $(r_1+s_1)^{-\frac12}$ repeated r_1+s_1 times and so multiplies a number of k by $(r_1+s_1)^{\frac12}$. Hence the rows R give a determinant

$$\delta^{\frac12} \prod_{j=1}^{s} (\tfrac12 i m_j n_j) \prod_{j=1}^{r} (r_j+s_j)^{\frac12}\, \nu^s$$

and so the determinant of the lattice $\mathscr{L}_3$ is

$$\det \mathscr{L}_1 \Big/ \left\{ \delta^{\frac12} \prod_{j=1}^{s} (\tfrac12 i m_j n_j) \prod_{j=1}^{r} (r_j+s_j)^{\frac12} \nu^s \right\}.$$

Now there is a point of $\mathscr{L}_3$ with sum of squares of coordinates positive and not greater than $\gamma_{N-n}(\det \mathscr{L}_2)^{2/N-n}$ and since the sum of squares of coordinates is

$$\sum_{j=1}^{r} \left\{ \sum_{i=1}^{r_j+s_j} \alpha_{j,i}{}^2 - \Big(\sum_i \alpha_{j,i}\Big)^2/(r_j+s_j) \right\} + \sum_{j=1}^{s} l_j{}^2 \left\{ \sum_{i=1}^{s_j} \beta_{j,i}{}^2 \right\} +$$
$$+ \sum_{j=1}^{s} m_j{}^2 \left\{ \sum_{i=1}^{\nu} \gamma_{j,i}{}^2 - \Big(\sum_i \gamma_{j,i}\Big)^2/\nu \right\} + \sum_{j=1}^{s} n_j{}^2 \left\{ \sum_{i=1}^{\nu} \varepsilon_{j,i}{}^2 - \Big(\sum_i \varepsilon_{j,i}\Big)^2/\nu \right\},$$

the result follows.

4. Some special cases of Theorem 1 have been proved already; in [2] we have $k=k(1)$, $l_1=1$ and in [3] we have $k=k(1)$, $N=4$, $r_1=2$, $s_1=1$, $l_1=(\sigma/3)^{\frac12}$. As has been stated in section 1 it was shown in [3] that a suitable choice of l_1 (and presumably, in general, of all l's, m's and n's) can improve the efficiency of the method by reducing the ratio of the largest discriminant to be considered to the chosen bound and hence possibly the ratio of the number of polynomials to be considered to the number which actually yield discriminants within the chosen bound.

5. As an example of the use of Theorem 1 I prove the following special result.

THEOREM 2. *The discriminant of a totally real sextic field, having* $k(5^{\frac12})$ *as a subfield, is either* 300125 *or is not less than* 355556. *Only the field* $K(5^{\frac12}, \cos(2\pi/7))$ *has the discriminant* 300125.

It seems likely that 300125 is the least possible value for the discriminant of a totally real sextic field.

PROOF. We take, in Theorem 1, $N=6$, $n=2$, $k=k(5^{\frac12})$, $\delta=5$, $r=2$, $r_1=r_2=3$, and $\Delta=355555$ and deduce that there exists a polynomial

$$P(x) = x^3 - (a+b\omega)x^2 + (c+d\omega)x - (e+f\omega)$$

with zeros α_{11}, α_{12}, α_{13} and a conjugate polynomial

$$\bar{P}(x) = x^3 - (a+b\bar{\omega})x^2 + (c+d\bar{\omega})x - (e+f\bar{\omega})$$

with zeros α_{21}, α_{22}, α_{23} such that

$$0 < {\alpha_{11}}^2+{\alpha_{12}}^2+{\alpha_{13}}^2 - \tfrac{1}{3}(\alpha_{11}+\alpha_{12}+\alpha_{13})^2 + {\alpha_{21}}^2+{\alpha_{22}}^2+{\alpha_{23}}^2 - \tfrac{1}{3}(\alpha_{21}+\alpha_{22}+\alpha_{23})^2 \leqq 2^{\frac{1}{2}}(\tfrac{1}{3}\cdot 71111^{\frac{1}{2}})^{\frac{1}{2}} < 40/3 .$$

(Throughout the proof $\omega = \frac{1}{2}(1+5^{\frac{1}{2}})$, $\bar{\omega} = \frac{1}{2}(1-5^{\frac{1}{2}})$ and $a, \ldots, h$ are rational integers.) Now

$${\alpha_{11}}^2+{\alpha_{12}}^2+{\alpha_{13}}^2 - \tfrac{1}{3}(\alpha_{11}+\alpha_{12}+\alpha_{13})^2 = \tfrac{2}{3}(a+b\omega)^2 - 2(c+d\omega)$$

and

$${\alpha_{21}}^2+{\alpha_{22}}^2+{\alpha_{23}}^2 - \tfrac{1}{3}(\alpha_{21}+\alpha_{22}+\alpha_{23})^2 = \tfrac{2}{3}(a+b\bar{\omega})^2 - 2(c+d\bar{\omega})$$

so that we need

$$(1) \qquad 0 < S = 2a^2+2ab+3b^2-3(2c+d) \leqq 19 .$$

Since all the zeros of $P(x)$ are real we have

$$(2) \quad \left(\tfrac{2}{27}(a+b\omega)^3 - \tfrac{1}{3}(a+b\omega)(c+d\omega)+e+f\omega\right)^2 \leqq \tfrac{4}{27}\left(\tfrac{1}{3}(a+b\omega)^2-c-d\omega\right)^3$$

and similarly

$$(3) \quad \left(\tfrac{2}{27}(a+b\bar{\omega})^3 - \tfrac{1}{3}(a+b\bar{\omega})(c+d\bar{\omega})+e+f\bar{\omega}\right)^2 \leqq \tfrac{4}{27}\left(\tfrac{1}{3}(a+b\bar{\omega})^2-c-d\bar{\omega}\right)^3 .$$

Hence we must have

$$\tfrac{1}{3}(a+b\omega)^2 - c-d\omega > 0$$

and

$$\tfrac{1}{3}(a+b\bar{\omega})^2 - c-d\bar{\omega} > 0$$

whence

$$(4) \quad (2c+d)/5^{\frac{1}{2}} - 2(a+b\bar{\omega})^2/3\ 5^{\frac{1}{2}} < d < 2(a+b\omega)^2/3\ 5^{\frac{1}{2}} - (2c+d)/5^{\frac{1}{2}} .$$

We do not affect the value of S, nor, apart from possibly interchanging conjugates, the field defined by the zeros if we add the same integer of $k(5^{\frac{1}{2}})$ to each zero, change ω into $\bar{\omega}$ or change the signs of the zeros. Hence we may suppose that a and b are each 1, 0 or -1, then that $b \geqq 0$, and finally exclude the cases $a=-1$, $b=0$ and $a=-1$, $b=1$ (because $-1+\bar{\omega}=-\omega$). Also if $a=b=0$ we may suppose that $d \geqq 0$ and $f \geqq 0$, and if $d=0$ that $e \geqq 0$, if $a=1$, $b=0$ that $d \geqq 0$, and if $d=0$ that $f \geqq 0$, and if $a=b=1$ that $d \geqq 1$, and if $d=1$ that $2e+f \geqq c$.

For each pair of values of (a, b) we find possible values of $2c+d$ from (1), then values of d from (4) and then (e, f) from (2) and (3). Finally we discard all polynomials which have a linear factor $x-g-h\omega$. We are left with the polynomials

$$\begin{aligned}
P_1(x) &= x^3-x^2-2x+1\,;\\
P_2(x) &= x^3-(1+\omega)x^2+(\omega-2)x+\omega\,;\\
P_3(x) &= x^3-x^2+(\omega-3)x-(\omega-2)\,;\\
P_4(x) &= x^3-\omega x^2-(\omega+2)x+\omega\,;\\
P_5(x) &= x^3-(1+\omega)x^2+(2\omega-3)x+2-\omega\,;\\
P_6(x) &= x^3-\omega x^2+(\omega-3)x+\omega\,;\\
P_7(x) &= x^3-\omega x^2+(\omega-3)x+\omega-1\,;\\
P_8(x) &= x^3-(1+\omega)x^2+(2\omega-3)x+\omega\,;\\
P_9(x) &= x^3-(1+\omega)x^2+(2\omega-3)x+1\,;\\
P_{10}(x) &= x^3-\omega x^2+(\omega-3)x+1\,;\\
P_{11}(x) &= x^3-3x+1.
\end{aligned}$$

The zeros of $P_1(x)$ are $-2\cos(2\pi/7)$, $-2\cos(4\pi/7)$, $-2\cos(6\pi/7)$, so that we obtain the field $K\big(5^{\frac{1}{2}}, \cos(2\pi/7)\big)$ with discriminant $5^3\cdot 7^4=300125$. $P_2(x)$ has discriminant $58+11\omega$ with norm 3881, and so its zeros give a field with discriminant $5^3\cdot 3881=485125$. Since

$$P_3(x) = -\frac{x^3}{\omega}\bar{P}_2\big(\bar{\omega}(x-1)/x\big)\,,$$

$$P_4(x) = -\frac{x^3}{\bar{\omega}}\bar{P}_2\big(\bar{\omega}(x-\omega)/x\big)\,,$$

$$P_5(x) = \frac{x^3}{\bar{\omega}}\bar{P}_2(\bar{\omega}/x)\,,$$

these give the same field as $P_2(x)$. Similarly $P_6(x)$ gives discriminant $5^3\cdot 7841=980125$, $P_7(x)$ and

$$P_8(x) = -\frac{(x-\omega)^3}{\omega}\bar{P}_7\big(1/(x-\omega)\big)$$

give discriminant $5^3\cdot 7729=966125$ and $P_9(x)$ gives discriminant $5^3\cdot 10501=1312625$. $P_{10}(x)$ has discriminant $104-36\omega$ with norm $5776=2^4\cdot 19^2$ and gives a field with discriminant $5^3\cdot 2^4\cdot 19^2=722000$. (The discriminant cannot be less than this since if so it would be at most $\frac{1}{4}\cdot 722000=180500$ and would yield a polynomial for which S was less than $\frac{3}{2}\cdot 2^{\frac{1}{2}}\cdot(\frac{1}{3}\cdot 36100^{\frac{1}{2}})^{\frac{1}{2}}=285^{\frac{1}{2}}=16.88\ldots$ whereas, for $P_{10}(x)$, S is 18.) Finally $P_{11}(x)$ has zeros $2\cos(2\pi/9)$, $2\cos(4\pi/9)$ and $2\cos(8\pi/9)$ and gives the field $K\big(5^{\frac{1}{2}}, \cos(2\pi/9)\big)$ with discriminant $5^3\cdot 3^8=820125$.

This completes the proof of Theorem 2.

REFERENCES

1. H. J. Godwin, *Real quartic fields with small discriminant,* J. London Math. Soc. 31 (1956), 478–485.
2. H. J. Godwin, *On totally complex quartic fields with small discriminants,* Proc. Cambridge Philos. Soc. 53 (1957), 1–4.
3. H. J. Godwin, *On quartic fields of signature one with small discriminant,* Quart. J. Math. Oxford Ser. (2) 8 (1957), 214–222.

UNIVERSITY COLLEGE OF SWANSEA, WALES