THE MINIMUM DISCRIMINANTS OF QUINTIC FIELDS

by JOHN HUNTER

(Received 6th January, 1956)

1. Introduction. Let D be the discriminant of an algebraic number field F of degree n over the rational field R. The problem of finding the lowest absolute value of D as F varies over all fields of degree n with a given number of real (and consequently of imaginary) conjugate fields has not yet been solved in general. The only precise results so far given are those for $n=2$, 3 and 4. The case $n=2$ is trivial ; $n=3$ was solved in 1896 by Furtwängler, and $n=4$ in 1929 by J. Mayer [6]. Reference to Furtwängler's work is given in Mayer's paper. In this paper the results for $n=5$, that is, for quintic fields, are obtained.

2. The fundamental theorem. Let F_1 be a quintic field, and let F_i $(i=2, 3, 4, 5)$ be the conjugate fields. If ρ_1 is an integer of F_1 we shall use ρ_i $(i=2, 3, 4, 5)$ to denote its conjugates and write $\Sigma\rho_i$ for $\rho_1+\rho_2+\rho_3+\rho_4+\rho_5$, etc. The method used is based on the following theorem

THEOREM 1. *If F_1 is a quintic field of discriminant D then we can write*

$$F_1=R(\rho_1),$$

where ρ_1 is an algebraic integer in F_1 such that

$$|\Sigma\rho_i|\leqslant 2,$$

and

$$5(\Sigma|\rho_i|^2)^4\leqslant 8|D|.$$

Proof. Let $(1, \rho_1', \theta_1', \phi_1', \psi_1')$ be an integral basis for the given field F_1, and $(1, \rho_1', \theta_i', \phi_i', \psi_i')$ the corresponding bases for the conjugate fields F_i $(i=2, 3, 4, 5)$. Write

$$f(x)=f(x_1, x_2, x_3, x_4, x_5)=\sum_{i=1}^{5}|x_1+\rho_i'x_2+\theta_i'x_3+\phi_i'x_4+\psi_i'x_5|^2$$

$$=\sum_{i=1}^{5}|X_i|^2,$$

say. Then $f(x)$ is a positive definite quadratic form of determinant $|D|$. For rational integers $x_1, \ldots, x_5$, the expressions X_i $(i=1, \ldots, 5)$ represent an algebraic integer of F_1 and its conjugates. Thus, for integral $(x)\neq(0)$, $\prod_{i=1}^{5}|X_i|\geqslant 1$, and hence $\sum_{i=1}^{5}|X_i|^2\geqslant 5$, by the inequality of the arithmetic-geometric means. Hence the minimum of the form $f(x)$ is 5, this being attained at the point (1, 0, 0, 0, 0).

We now define successive minima m_1, m_2, m_3, m_4, m_5 of $f(x)$ as follows :

m_1 is the minimum of $f(x)$ for all integral $(x)\neq(0)$, so that $m_1=5$ and is attained at the point $(x_1)=(1, 0, 0, 0, 0)$;

m_2 is the minimum of $f(x)$ for all integral (x) not proportional to (x_1), attained at (x_2), say ;

m_3 is the minimum of $f(x)$ for all integral (x) not linearly dependent on (x_1) and (x_2), attained at (x_3), say ; and so on. Then clearly

$$5=m_1\leqslant m_2\leqslant m_3\leqslant m_4\leqslant m_5. \tag{1}$$

Also it has been proved that

$$m_1m_2m_3m_4m_5 \leqslant \gamma_5^5 \mid D \mid,$$

(since $| D |$ is the determinant of $f(x)$), where γ_5 is the "minimum" of all positive definite quadratic forms in five integral variables. Since $\gamma_5 = \sqrt[5]{8}$, we obtain

$$m_1m_2m_3m_4m_5 \leqslant 8 \mid D \mid. \tag{2}$$

By (1) and (2),

$$5m_2^4 \leqslant 8 \mid D \mid. \tag{3}$$

Let

$$\begin{aligned} f(x) &= 5x_1^2 + 2b_{12}x_1x_2 + \ldots + 2b_{15}x_1x_5 + b_{22}x_2^2 + \ldots \\ &= 5\left(x_1 + \frac{b_{12}}{5}x_2 + \ldots + \frac{b_{15}}{5}x_5\right)^2 + g(x_2, x_3, x_4, x_5) \\ &= 5\xi^2 + g(x_2, x_3, x_4, x_5), \end{aligned}$$

so that g is a positive definite quadratic form in the variables x_2, x_3, x_4, x_5. Now suppose that

$$m_2 = f(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5).$$

By definition of m_2, $\alpha_2, \ldots, \alpha_5$ are not all zero, since m_1 arises at the point (1, 0, 0, 0, 0). Write

$$\delta = \text{g.c.d.}(\alpha_2, \alpha_3, \alpha_4, \alpha_5).$$

We show that $\delta = 1$. Suppose not; then we can take $\delta \geqslant 2$ and, putting $\alpha_i = \delta\beta_i (i = 2, \ldots, 5)$, we have

$$m_2 = f(\alpha) = 5\xi^2(\alpha) + \delta^2 g(\beta).$$

Now let $m_2' = \min f(x)$, under the condition that $x_i = \beta_i (i = 2, \ldots, 5)$ are fixed. Then, since not all the β_i are zero, it is clear that

$$m_2 \leqslant m_2'.$$

Suppose that

$$m_2' = f(\gamma, \beta_2, \ldots, \beta_5) = 5\{\gamma + \tfrac{1}{5}\sum_{i=2}^{5} b_{1i}\beta_i\}^2 + g(\beta).$$

Now, given any set of integers $(\beta_2, \ldots, \beta_5)$, we can always choose an integer γ such that

$$\left| \gamma + \tfrac{1}{5}\sum_{i=2}^{5} b_{1i}\beta_i \right| \leqslant \tfrac{1}{2}.$$

Thus, from the definition of m_2',

$$m_2' \leqslant \tfrac{5}{4} + g(\beta).$$

Hence

$$\delta^2 g(\beta) \leqslant 5\xi^2(\alpha) + \delta^2 g(\beta) = m_2 \leqslant m_2' \leqslant \tfrac{5}{4} + g(\beta).$$

Thus

$$(\delta^2 - 1)g(\beta) \leqslant \tfrac{5}{4},$$

so that

$$g(\beta) \leqslant \tfrac{5}{12},$$

since $\delta \geqslant 2$. It follows that $m_2 \leqslant \frac{5}{4} + \frac{5}{12} = \frac{5}{3}$. But $m_2 \geqslant 5$. Hence we have a contradiction, and therefore $\delta = 1$. Thus

$$m_2 = f(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5),$$

where g.c.d.$(\alpha_2, \alpha_3, \alpha_4, \alpha_5) = 1$. Now, since g.c.d.$(\alpha_2, \alpha_3, \alpha_4, \alpha_5) = 1$, we can find a 4×4 integral matrix

$$\begin{pmatrix} \alpha_2 & \beta_2 & \gamma_2 & \delta_2 \\ \alpha_3 & \beta_3 & \gamma_3 & \delta_3 \\ \alpha_4 & \beta_4 & \gamma_4 & \delta_4 \\ \alpha_5 & \beta_5 & \gamma_5 & \delta_5 \end{pmatrix}.$$

https://doi.org/10.1017/S2040618500033463 Published online by Cambridge University Press

of determinant 1 (the (β_i) and γ_5 are not related to the (β_i) and γ_5 above). Put

$$x_1 = x_1' + \alpha_1 x_2',$$
$$x_i = \alpha_i x_2' + \beta_i x_3' + \gamma_i x_4' + \delta_i x_5' \quad (i = 2, \ldots, 5).$$

This is an integral unimodular substitution. Applying it to $f(x)$, we have

$$f(x) = \sum_{i=1}^{5} | x_1' + (\alpha_1 + \rho_i'\alpha_2 + \theta_i'\alpha_3 + \phi_i'\alpha_4 + \psi_i'\alpha_5)x_2' + (\quad)x_3' + \ldots |^2,$$
$$= \sum_{i=1}^{5} | x_1 + \rho_i x_2 + \theta_i x_3 + \phi_i x_4 + \psi_i x_5 |^2,$$

say, dropping the dashes from the x_i'. Since the substitution is integral and unimodular follows that $(1, \rho_1, \theta_1, \phi_1, \psi_1)$ is an integral basis for F_1 and that $(1, \rho_i, \theta_i, \phi_i, \psi_i)$, $i = 2, 3, 4, 5$, are the corresponding bases for the conjugate fields. Now, if

$$f(x) = \sum_{i,j=1}^{5} b_{ij} x_i x_j,$$

then $b_{11} = 5$, $b_{22} = \Sigma | \rho_i |^2$, and

$$2b_{12} = \Sigma(\rho_i + \bar{\rho}_i) = \Sigma\rho_i + \overline{\Sigma\rho_i} = 2\Sigma\rho_i,$$

since $\Sigma\rho_i$ is a rational integer. Also, by the above substitution, $(x) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ corresponds to $(x') = (0, 1, 0, 0, 0)$. Hence

$$m_2 = \Sigma | \rho_i |^2 = b_{22}.$$

Thus, by (3),

$$5(\Sigma | \rho_i |^2)^4 \leqslant 8 | D | .$$

Now, from the equations for $x_2, \ldots, x_5$ in terms of $x_2', \ldots, x_5'$ it follows that $(x_2, \ldots, x_5) = (0, \ldots, 0)$ if and only if $(x_2', \ldots, x_5') = (0, \ldots, 0)$. Thus, taking $x_1 = 1$, $x_2 = \pm 1$, $x_3 = x_4 = x_5 = 0$, in the simplified notation, we have, from the definition of m_2,

$$b_{11} + 2b_{12} + b_{22} \geqslant b_{22},$$
$$b_{11} - 2b_{12} + b_{22} \geqslant b_{22}.$$

Therefore
$$| b_{12} | \leqslant \tfrac{1}{2} b_{11},$$
and so
$$| \Sigma \rho_i | \leqslant \tfrac{5}{2}.$$

Hence, since $\Sigma\rho_i$ is a rational integer, $| \Sigma\rho_i | = 0$, 1 or 2.

We have now shown that there is an integer ρ_1 in F_1, not a rational integer, such that the inequalities in the statement of Theorem 1 hold. Hence, since a quintic field has no non-trivial subfields, $F_1 = R(\rho_1)$ and the result follows.

We note that the same proof establishes the corresponding result in which " quintic field " is replaced by " number field of degree $n \leqslant 14$ with no non-trivial subfields."

3. Totally real quintic fields. Let F_1 be a totally real quintic field of discriminant D; then $D > 0$. By Theorem 1, we can assume that $F_1 = R(\rho_1)$, where ρ_1 is an algebraic integer in F_1 such that

$$| \Sigma\rho_i | = 0, 1, \text{ or } 2, \tag{4}$$

and

$$5(\Sigma | \rho_i |^2)^4 \leqslant 8D. \tag{5}$$

Since the ρ_i are all real and $\Sigma\rho_i^2$ is a rational integer, (5) gives

$$\Sigma\rho_i^2 \leqslant [(\tfrac{8}{5}D)^{\frac{1}{4}}], \tag{6}$$

where the expression on the right is the integral part of $(\frac{8}{5}D)^{\frac{1}{4}}$. Let

$$g(x) \equiv x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0 \tag{7}$$

be the irreducible equation for ρ_1 over R, so that, by the definition of an integer in an algebraic field, the a_i are rational integers. Also, since ρ_2, ρ_3, ρ_4, ρ_5 are the conjugates of ρ_1, the roots of (7) are $\rho_1, \ldots, \rho_5$. Thus $\Sigma\rho_i = -a_1$. Hence, from (4), by replacing ρ_i by $-\rho_i$ if necessary, we can suppose that

$$a_1 = 0, 1, \text{ or } 2. \tag{8}$$

Since $\Pi\rho_i$ is a non-zero rational integer we have $|\Pi\rho_i| \geqslant 1$, and thus, using the inequality of the arithmetic-geometric means,

$$1 \leqslant |\Pi\rho_i| \leqslant (\tfrac{1}{5}\Sigma\rho_i^2)^{\frac{5}{2}}.$$

Hence, from (6),

$$5 \leqslant \Sigma\rho_i^2 \leqslant [(\tfrac{8}{5}D)^{\frac{1}{4}}].$$

Now $\Sigma\rho_i^2 = 5$, $|\Pi\rho_i| \geqslant 1$ together imply that $\rho_i^2 = 1$ $(i = 1, \ldots, 5)$, and so that $g(x)$ is reducible. Thus

$$6 \leqslant \Sigma\rho_i^2 \leqslant [(\tfrac{8}{5}D)^{\frac{1}{4}}]. \tag{9}$$

Since $(\Sigma\rho_i)^2 = \Sigma\rho_i^2 + 2\Sigma\rho_i\rho_j$ and $\Sigma\rho_i\rho_j = a_2$ we deduce, from (9), that

$$-\tfrac{1}{2}([(\tfrac{8}{5}D)^{\frac{1}{4}}] - a_1^2) \leqslant a_2 \leqslant -\tfrac{1}{2}(6 - a_1^2). \tag{10}$$

From (8) and (10) it follows that a_2 must be negative. An inequality for a_5 is given by

$$|a_5| = |\Pi\rho_i| \leqslant [(\tfrac{1}{5}\Sigma\rho_i^2)^{\frac{5}{2}}], \tag{11}$$

so that the values of a_5 which can arise are obtained by inserting in (11) the possible values of $\Sigma\rho_i^2$ given by (9).

An inequality for a_3 can be obtained by using the fact that, if $g(x) = 0$ has five distinct real roots, then $g''(x) = 0$ must have three distinct real roots and so its discriminant must be positive. The inequality, which involves a_1 and a_2, is

$$|a_3 - \tfrac{1}{25}(15a_1a_2 - 4a_1^3)| < \tfrac{1}{25}(2a_1^2 - 5a_2)\sqrt{(4a_1^2 - 10a_2)}. \tag{12}$$

The above discussion shows that any totally real quintic field F_1 of given discriminant D can be written as $R(\rho_1)$, where ρ_1 is an algebraic integer whose irreducible equation (7) is such that a_1, a_2, a_3, a_5 satisfy (8), (10), (12) and (11). We now take $D = 14641$, the discriminant of the field defined by a root of the equation

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0,$$

and shall show eventually that this is in fact the minimum discriminant of totally real quintic fields. That 14641 is the discriminant of this field follows from Lemma 1 below and the following facts :

(i) The discriminant of the equation is $14641 = 11^4$. (ii) From (9) we obtain $[(\frac{8}{5}D)^{\frac{1}{4}}] \geqslant 6$, and thus $D \geqslant 810$. This is an improvement on Minkowski's result, $D \geqslant (5^5/5!)^2$, which gives $D \geqslant 679$.

LEMMA 1. *If the integer ρ of a quintic field F_1 of discriminant D satisfies no equation of degree less than five with rational coefficients, then, if D_ρ is the discriminant of the irreducible equation of degree five satisfied by ρ,*

$$D_\rho = d^2D,$$

where d is a rational integer.

This is a particular case of a well-known result [4(*a*)].

In the above case $D_\rho = 14641 = (11)^2 \,.\, 121 = (121)^2 \,.\, 1$ and hence the only possibility is $D_\rho = D = 14641$, since the equation is irreducible and $810 > 121 > 1$.

https://doi.org/10.1017/S2040618500033463 Published online by Cambridge University Press

With the above value of D, and noting that if $a_1=0$ we can, by changing ρ_i into $-\rho_i$ if necessary, ensure that $a_3 \geqslant 0$, we now have, from (8), (9), (10), (11) and (12), the following ranges for a_1, a_2, a_3, with corresponding first approximations to ranges of possible values of a_5 :

a_1	a_2	a_3	$\lvert a_5 \rvert \leqslant$
0	−6	[0, 9]	8
0	−5	[0, 7]	5
0	−4	[0, 5]	3
0	−3	[0, 3]	1
1	−5	[−11, 4]	7
1	−4	[−8, 3]	4
1	−3	[−5, 2]	2
2	−4	[−14, 2]	8
2	−3	[−11, 1]	5
2	−2	[−7, 0]	3
2	−1	[−5, 0]	1

(13)

where, for example in the case $a_1=0$, $a_2=-6$, a_3 runs through the interval $0 \leqslant a_3 \leqslant 9$, and a_5 the interval $\lvert a_5 \rvert \leqslant 8$ with $a_5=0$ omitted.

We now proceed to apply a succession of inequalities for a_4 and a_5 which at the same time considerably reduce the ranges of values for a_1, a_2, a_3 given in (13). We note first that necessary conditions for equation (7) to have five real roots are given by Newton's inequalities [3] :

$$\text{(i) } a_2 < \tfrac{2}{5}a_1^2, \quad \text{(ii) } a_1a_3 < \tfrac{1}{2}a_2^2, \quad \text{(iii) } a_2a_4 < \tfrac{1}{2}a_3^2, \quad \text{(iv) } a_3a_5 < \tfrac{2}{5}a_4^2,$$

with strict inequality since the ρ_i must be distinct. Of these, (i) and (ii) give no new information, (iii) gives $a_4 > -\dfrac{1}{2\lvert a_2 \rvert}a_3^2$, and (iv) we shall use later.

Another inequality for a_4 is obtained from the fact that the discriminant of $g'(x)=0$ must be positive. On reduction, this inequality can be expressed in the form

$$K \equiv 2000a_4^3 + A_1a_4^2 + A_2a_4 + A_3 > 0, \tag{14}$$

where

$$A_1 = (2160a_1^2a_2 - 1800a_2^2 - 432a_1^4) - 2400a_1a_3,$$

$$A_2 = (405a_2^4 - 108a_1^2a_2^3) + (432a_1^3a_2 - 1800a_1a_2^2)a_3 + (2700a_2 - 120a_1^2)a_3^2,$$

$$A_3 = (36a_1^2a_2^2 - 135a_2^3)a_3^2 + (540a_1a_2 - 128a_1^3)a_3^3 - 675a_3^4.$$

As an aid in the application of this inequality for a_4 we obtain, by the following lemma, a simpler one-sided inequality for a_4.

LEMMA 2. *A set of necessary and sufficient conditions for $g(x)=0$ to have five real roots is that the following symmetric determinant and its principal minors be positive, viz.*

$$D' = \begin{vmatrix} 4a_1^2 - 10a_2 & 3a_1a_2 - 15a_3 & 2a_1a_3 - 20a_4 & a_1a_4 - 25a_5 \\ 3a_1a_2 - 15a_3 & 6a_2^2 - 10a_1a_3 - 20a_4 & 4a_2a_3 - 15a_1a_4 - 25a_5 & 2a_2a_4 - 20a_1a_5 \\ 2a_1a_3 - 20a_4 & 4a_2a_3 - 15a_1a_4 - 25a_5 & 6a_3^2 - 10a_2a_4 - 20a_1a_5 & 3a_3a_4 - 15a_2a_5 \\ a_1a_4 - 25a_5 & 2a_2a_4 - 20a_1a_5 & 3a_3a_4 - 15a_2a_5 & 4a_4^2 - 10a_3a_5 \end{vmatrix}$$

Also

$$D_{\rho_1} = D'/5^3,$$

in the notation of Lemma 1.

https://doi.org/10.1017/S2040618500033463 Published online by Cambridge University Press

Proof. Let $(\alpha_1, \ldots, \alpha_5)$ be a set of roots of the equation $g(x)=0$, so that $\Sigma\alpha_i = -a_1$, etc.

Let
$$\Phi(x_0, x_1, x_2, x_3, x_4) = \sum_{i=1}^{5} (x_0 + \alpha_i x_1 + \alpha_i^2 x_2 + \alpha_i^3 x_3 + \alpha_i^4 x_4)^2.$$

Then, it is known [5(*a*)] that on reducing this real quadratic form in $x_0, \ldots, x_4$ to canonical form by a real linear transformation, the number of squares with negative coefficient is equal to the number of pairs of complex roots of $g(x)=0$. Hence $g(x)=0$ has five real roots if and only if Φ is positive definite. Writing $s_\nu = \Sigma\alpha_i^\nu$, we have

$$5\Phi = (5x_0 + s_1x_1 + s_2x_2 + s_3x_3 + s_4x_4)^2 + h(x_1, x_2, x_3, x_4), \tag{15}$$

where
$$h(x_1, x_2, x_3, x_4) = \sum_{i,j=1}^{4} a_{ij}x_ix_j,$$

with
$$a_{ij} = 5s_{i+j} - s_is_j.$$

Clearly $g(x)=0$ has five real roots if and only if h is positive definite.

We now apply the integral unimodular substitution

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 & a_1 & a_2 & a_3 \\ 0 & 1 & a_1 & a_2 \\ 0 & 0 & 1 & a_1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \xi_4 \end{pmatrix}$$

of determinant 1, and use the usual relations

$$\sum_{i=0}^{5} a_is_{r-i} = 0 \quad (r = 1, 2, \ldots, 8),$$

where $a_0 = 1$, $s_0 = r$ when $r \leqslant 5$ and $s_i = 0$ when $i < 0$, giving the s_ν in terms of the a_ν. By direct calculation, we find that

$$h(x_1, x_2, x_3, x_4) = h'(\xi_1, \xi_2, \xi_3, \xi_4) = \sum_{i,j=1}^{4} a'_{ij}\xi_i\xi_j,$$

where (a'_{ij}) is the 4×4 matrix whose determinant is given in the enunciation of the lemma. Hence $g(x)=0$ has five real roots if and only if h' is positive definite, that is, if and only if (a'_{ij}) is positive definite, which is the required result.

Also, the determinant of Φ is

$$\begin{aligned} &|\alpha_i^\nu|^2 \quad (\nu = 0, \ldots, 4\,;\, i = 1, \ldots, 5) \\ &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= D_{\rho_1}. \end{aligned}$$

Hence, comparing the determinants of the quadratic forms on each side of the identity (15) we have

$$D_{\rho_1} = D'/5^3.$$

This lemma provides four conditions for $g(x)=0$ to have five real roots:

(i) $4a_1^2 - 10a_2 > 0$, which is automatically satisfied;

(ii) $\begin{vmatrix} 4a_1^2 - 10a_2, & 3a_1a_2 - 15a_3 \\ 3a_1a_2 - 15a_3, & 6a_2^2 - 10a_1a_3 - 20a_4 \end{vmatrix} > 0,$

which, with
$$a_4 > -\frac{1}{2\,|\,a_2\,|}\,a_3^2,$$

https://doi.org/10.1017/S2040618500033463 Published online by Cambridge University Press

gives $$-\frac{1}{2\,|\,a_2\,|}\,a_3^2 < a_4 < \frac{1}{10}\,(3a_2^2 - 5a_1a_3) - \frac{9}{40}\cdot\frac{(a_1a_2 - 5a_3)^2}{2a_1^2 - 5a_2}\,; \tag{16}$$

(iii) $$\begin{vmatrix} 4a_1^2 - 10a_2, & 3a_1a_2 - 15a_3, & 2a_1a_3 - 20a_4 \\ 3a_1a_2 - 15a_3, & 6a_2^2 - 10a_1a_3 - 20a_4, & 4a_2a_3 - 15a_1a_4 - 25a_5 \\ 2a_1a_3 - 20a_4, & 4a_2a_3 - 15a_1a_4 - 25a_5, & 6a_3^2 - 10a_2a_4 - 20a_1a_5 \end{vmatrix} > 0,$$

that is, $$Y \equiv B_1a_5^2 + 2B_2a_5 + B_3 > 0, \tag{17}$$

where
$$B_1 = -25\,(2a_1^2 - 5a_2),$$
$$B_2 = C + Da_4,$$
$$B_3 = E + Fa_4 + Ga_4^2 + 160a_4^3,$$

and
$$C = (12a_1a_2^3 - 3a_1^3a_2^2) + (8a_1^4 - 33a_1^2a_2^2 - 20a_2^2)a_3 + 60a_1a_3^2,$$
$$D = 65a_1a_2 - 14a_1^3 - 150a_3,$$
$$E = (a_1^2a_2^2 - 4a_2^3)a_3^2 + (18a_1a_2 - 4a_1^3)a_3^3 - 27a_3^4,$$
$$F = (12a_2^4 - 3a_1^2a_2^3) + (14a_1^3a_2 - 62a_1a_2^2)a_3 + (117a_2 - 6a_1^2)a_3^2,$$
$$G = 97a_1^2a_2 - 18a_1^4 - 88a_2^2 - 132a_1a_3\,;$$

(iv) $D' > 0$.

To assist in reducing the number of possibilities for a_5, we use another necessary condition for $g(x) = 0$ to have five real roots which can be easily applied, and which arises from work of Hermite [5(*b*)]. This involves the discriminant of a quadratic covariant of the equation and, on simplification, leads to the inequality

$$X \equiv 625a_5^2 + 5H_1a_5 + H_2 < 0, \tag{18}$$

where $$H_1 = (-3a_1a_2^2 + 8a_1^2a_3 + 5a_2a_3) - 50a_1a_4,$$
and $$H_2 = (6a_1a_3^3 - 2a_2^2a_3^2) + (6a_2^3 - 15a_3^2 - 19a_1a_2a_3)a_4 + (9a_1^2 + 40a_2)a_4^2.$$

We can now apply, as follows, the inequalities which have been established for a_4 and a_5. Using the ranges for a_1, a_2 and a_3 given in (13), we first obtain, systematically, the values of a_4 which satisfy both (14) and (16) (in some cases there are no values). The possible values of a_5, corresponding to each of the possible sets of values of a_1, a_2, a_3 and a_4, are now obtained by applying (18), using the condition $a_3a_5 < 2a_4^2/5$ wherever possible and then applying (17). Many of the remaining equations are reducible, containing either a rational linear or a rational quadratic factor, and so can be eliminated. At this stage we find that none of the values of a_1 and a_2 in the set $(a_1, a_2) = (0, -3), (0, -4), (1, -3), (2, -1)$ and $(2, -2)$ gives an irreducible equation with five real roots, and that the ranges of possible values of a_3, a_4 and a_5 for the other pairs of values of a_1 and a_2 are very considerably reduced.

To the equations which remain we have now to apply the condition $D' > 0$ and, for those satisfying this condition, determine $D_{\rho_1} = D'/5^3$. These operations can be combined by using

$$D_{\rho_1} = 3125a_5^4 + H_1a_5^3 + H_2a_5^2 + H_3a_5 + H_4, \tag{19}$$

where
$$H_1 = P_1 + P_2a_4,$$
$$H_2 = Q_1 + Q_2a_4 + Q_3a_4^2,$$
$$H_3 = R_1 + R_2a_4 + R_3a_4^2 + R_4a_4^3,$$
$$H_4 = S_1a_4^2 + S_2a_4^3 + S_3a_4^4 + 256a_4^5,$$

and $P_1=(256a_2^5+2250a_1a_2^3-1600a_1^3a_2)+(2000a_1^2-3750a_2)a_3,$

$P_2=-2500a_1,$

$Q_1=(108a_2^5-27a_1^2a_2^4)+(144a_1^3a_2^2-630a_1a_2^3)a_3+(560a_1^2a_2-128a_1^4+825a_2^2)a_3^2-900a_1a_3^3,$

$Q_2=(1020a_1^2a_2^2-192a_1^4a_2-900a_2^3)+(160a_1^3-2050a_1a_2)a_3+2250a_3^2,$

$Q_3=-50a_1^2+2000a_2,$

$R_1=(16a_2^3-4a_1^2a_2^2)a_3^2+(16a_1^3-72a_1a_2)a_3^4+108a_3^5,$

$R_2=(18a_1^2a_2^3-72a_2^4)a_3+(356a_1a_2^2-80a_1^3a_2)a_3^2+(24a_1^2-630a_2)a_3^3,$

$R_3=(24a_1a_2^3-6a_1^3a_2^2)+(144a_1^4-746a_1^2a_2+560a_2^2)a_3+1020a_1a_3^2,$

$R_4=(160a_1a_2-36a_1^3)-1600a_3,$

$S_1=(a_1^2a_2^2-4a_2^3)a_3^2+(18a_1a_2-4a_1^3)a_3^3-27a_3^4,$

$S_2=(16a_2^4-4a_1^2a_2^3)+(18a_1^3a_2-80a_1a_2^2)a_3+(144a_2-6a_1^2)a_3^2,$

$S_3=(144a_1^2a_2-128a_2^2-27a_1^4)-192a_1a_3.$

On examining first the three simplest cases $(a_1, a_2)=(0, -5)$, $(1, -4)$ and $(2, -3)$, we are left with the irreducible equations of positive discriminant given in the following table :

a_1	a_2	a_3	a_4	a_5	D_{ρ_1}
0	−5	0	4	1	38569
0	−5	1	3	−1	24217
0	−5	1	5	−1	24217
1	−4	−3	3	1	14641
2	−3	−4	2	1	24217
2	−3	−5	1	1	36497
2	−3	−6	0	1	24217.

Using Lemma 1, we easily see that each of these discriminants is also the discriminant of the corresponding algebraic number field.

From the three remaining cases $(a_1, a_2)=(0, -6)$, $(1, -5)$ and $(2, -4)$, 54 equations are left, and are such that the corresponding equation discriminants are not less than 24217. We have now to show that there is no corresponding field discriminant less than 14641. For the cases $(a_1, a_2)=(0, -6)$ and $(2, -4)$, $\Sigma\rho_i^2=a_1^2-2a_2=12$. Hence, by (6), these cases can arise only if $D\geqslant\frac{5}{8}.\,12^4=12960$. Thus, in these two cases, by Lemma 1, only those equation discriminants have to be considered, which can be written as d^2A, where A is an integer such that $12960\leqslant A\leqslant 14641$, and d is any integer greater than 1. Similarly, in the case $(a_1, a_2)=(1, -5)$, the corresponding range for A is $9151\leqslant A\leqslant 14641$. Only the four equations given in the following table arise for further discussion :

a_1	a_2	a_3	a_4	a_5	$D\rho_1$
0	−6	2	6	−2	$4^2 . 13997=2^4 . 13997$
2	−4	−5	3	1	$4^2 . 13658=2^5 . 6829$
2	−4	−6	2	2	$4^2 . 13989=2^4 . 3 . 4663$
2	−4	−6	3	2	$4^2 . 14389=2^4 . 14389.$

The entries in the last column give the prime-factorisations of the discriminants. To determine the powers of 2 in the corresponding field discriminants we use the known result [4(*b*)] :

Lemma 3. *If* $p=\prod_{i=1}^{s}\mathfrak{p}_i^{e_i}$ *is the representation of prime* p *in terms of its prime divisors in the*

https://doi.org/10.1017/S2040618500033463 Published online by Cambridge University Press

algebraic number field $R(\rho)$ *and the degree of* $\mathfrak{p}_i$ *is* f_i, *then the power*, $D_{\mathfrak{p}}$, *of* p *contained in the discriminant of the field* $R(\rho)$ *is given by*

$$D_{\mathfrak{p}} = \prod_{i=1}^{s} p^{f_i(\overline{e_i}-1)},$$

where $\overline{e_i} = e_i$ *if* $p \nmid e_i$ *and* $e_i + 1 \leqslant \overline{e_i} \leqslant (r_i+1)e_i$ *if* $p \mid e_i$, p^{r_i} *being the power of* p *in* e_i.

The representation of 2 in terms of its prime divisors is obtained very simply by the method described in Berwick's *Integral Bases* [1]. The second dissection criterion of Chapter VII applies in each of the four cases and, with Lemma 3, shows that the field discriminants are all greater than 14641.

Combining the results obtained in this section we have :

THEOREM 2. *The minimum discriminant of totally real quintic fields is* 14641, *the corresponding field being* $R(\rho)$, *where* ρ *is a root of the equation*

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0.$$

The equation is the cyclotomic equation whose roots are the binomial periods $\alpha_i + 1/\alpha_i$, the α_i being the primitive 11th roots of unity.

We note that it appears likely that the second minimum is 24217, the field being defined by the equation $x^5 - 5x^3 + x^2 + 3x - 1 = 0$. Other small discriminants of totally real quintic fields are 36497, 38569, 65657, 70601, 81509, 81589, 89417, 101833, ...

4. Quintic fields with one real and four imaginary conjugate fields. We first note that the field defined by the irreducible equation $x^5 - x^3 + x^2 + x - 1 = 0$ has discriminant 1609 and hence, by Theorem 2, must have one real and four imaginary conjugate fields.

Proceeding as in § 3, using Theorem 1 and taking $D = 1609$, we find that any field of the type under discussion of discriminant not exceeding 1609 can be represented as $R(\rho_1)$, where ρ_1 is an algebraic integer such that, in the notation of § 3,

$$a_1 = -\Sigma\rho_i = 0, 1 \text{ or } 2, \quad 5 < \Sigma \mid \rho_i \mid^2 \leqslant 7{\cdot}123\ldots,$$

and $\mid a_5 \mid \leqslant 2$. For simplicity of notation we write ρ, $\sigma \pm i\tau$, $\alpha \pm i\beta$, where ρ, σ, τ, α and β are real, for the one real and four complex conjugates of ρ_1, so that $\Sigma\rho_i = \rho + 2\sigma + 2\alpha = -a_1$, $\Sigma \mid \rho_i \mid^2 = \rho^2 + 2(\sigma^2 + \alpha^2 + \tau^2 + \beta^2)$, $a_2 = \frac{1}{2}(a_1^2 - U)$ where $U = \Sigma\rho_i^2 = \rho^2 + 2(\sigma^2 + \alpha^2 - \tau^2 - \beta^2)$, etc. The ranges of values of a_2 are given by the following lemma :

LEMMA 4. *If* $$U = \rho^2 + 2(\sigma^2 + \alpha^2 - \tau^2 - \beta^2),$$
where $$\rho^2 + 2(\sigma^2 + \alpha^2 + \tau^2 + \beta^2) = a,$$
and $$\rho + 2\sigma + 2\alpha = b,$$
then $$-(a - 2b^2/5) \leqslant U \leqslant a,$$
provided that $5a - b^2 > 0$.

The Lagrangian method can be applied and gives the result fairly easily. This leads to the following inequalities for a_2 :

$$a_1 = 0 \ : \ -3 \leqslant a_2 \leqslant 3\ ,$$
$$a_1 = 1 \ : \ -3 \leqslant a_2 \leqslant 3\ ,$$
$$a_1 = 2 \ : \ -1 \leqslant a_2 \leqslant 4\ .$$

By considering the function $\Sigma\rho_i^3$ under the restrictions on $\Sigma\rho_i$, $\Sigma \mid \rho_i \mid^2$ and $\Sigma\rho_i^2$, the solution of a much more complicated maximum and minimum problem leads to the following ranges for a_3 :

$a_1=0$		$a_1=1$		$a_1=$	
a_2	a_3	a_2	a_3	a_2	a_3
-3	$[0, 4]$	-3	$[-6, 2]$	-1	$[-5, 0]$
-2	$[0, 3]$	-2	$[-5, 2]$	0	$[-4, 1]$
-1	$[0, 3]$	-1	$[-4, 2]$	1	$[-3, 3]$
0	$[0, 3]$	0	$[-3, 3]$	2	$[-1, 4]$
1	$[0, 3]$	1	$[-3, 3]$	3	$[0, 5]$
2	$[0, 3]$	2	$[-2, 4]$	4	$[1, 6]$.
3	$[0, 2]$	3	$[-1, 4]$		

For a_4 the use of $\Sigma\rho_i^2$ proves to be much too complicated. By considering a_4 itself under the restrictions on $\Sigma\rho_i$ and $\Sigma\,|\,\rho_i\,|^2$ we obtain, again by a complicated discussion, the ranges:

$$a_1=0\ :\ -3\leqslant a_4\leqslant 3,$$
$$a_1=1\ :\ -4\leqslant a_4\leqslant 4,$$
$$a_1=2\ :\ -5\leqslant a_4\leqslant 5.$$

In this case there is no simple sequence of inequalities such as that used in § 3. We have to deal directly with D_{ρ_1} as given in (19) and, fixing a_1, a_2, a_3 and a_5, use the condition $D_{\rho_1}>0$ to determine a_4 and at the same time D_{ρ_1}. The following lemma gives some help in this work.

LEMMA 5. *If the irreducible equation*

$$g(x)\equiv x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5=0$$

has one real and four complex roots, then,

$$\textit{if } a_5>0,\ \textit{either}\ a_3>-a_1-a_5\ \textit{or}\ a_4>-a_2-1,$$

and

$$\textit{if } a_5<0,\ \textit{either}\ a_3<-a_1-a_5\ \textit{or}\ a_4>-a_2-1.$$

This follows easily by considering $g(0)$, $g(1)$ and $g(-1)$.

The smallest equation discriminant (of an irreducible equation) which appears is 1609, this being also the discriminant of the corresponding number fields. By using first Lemma 1 with suitable values for A, in the notation of § 3, and then applying Lemma 3 with Berwick's second dissection, it can be shown that all except eight of the other irreducible equations define fields of discriminant not less than 1609. Using either a suitable transformation of variable or Berwick's third dissection or by finding an integral basis for the field defined by the equation (Berwick, Chapter IX), we find that these eight equations define fields of discriminant greater than 1609.

There are ten equations defining fields with discriminant 1609. They are given by:

a_1	a_2	a_3	a_4	a_5
0	-3	0	2	1
0	-1	1	1	-1
1	-1	-1	0	1
1	3	3	2	1
2	0	-3	0	1
2	1	-2	-2	-1
2	2	-1	-2	-1
2	3	3	1	1
2	3	3	3	1
2	3	5	3	-1,

https://doi.org/10.1017/S2040618500033463 Published online by Cambridge University Press

the first nine having equation discriminant 1609 and the tenth equation discriminant $78841 = 7^2 . 1609$. Denoting the roots of these equations by $x_1, \rho, x_2, \ldots, x_9$, respectively, we have

$$x_1 = 1/x_4 = -\rho^4 - \rho^3 - 1, \qquad x_2 = -1/\rho,$$
$$x_7 = 1/x_3 = -\rho^3 - 1, \qquad x_5 = 1/x_6 = 1/\rho^2 - 1,$$
$$x_8 = -\rho^2, \qquad x_9 = \rho^4.$$

Hence these equations define the same field.

Thus, from the results of this section we have :

THEOREM 3. *The minimum discriminant of quintic fields with one real and four imaginary conjugate fields is* 1609, *the corresponding field being* $R(\rho)$, *where* ρ *is a root of the equation*

$$x^5 - x^3 + x^2 + x - 1 = 0.$$

From the work, it appears likely that the second minimum is 1649, the corresponding field being defined by the equation $x^5 + x^4 - x^2 - x + 1 = 0$. The succeeding minima appear to be 1777, 2209, 2297, 2617, 2665, 2869, 3017, 3089, ... The method in fact provides quite an extensive table of quintic fields of the type under discussion with their discriminants.

5. Quintic fields with three real and two imaginary conjugate fields. The method used in this case was identical with that used in § 4. Since no new problems arise we shall simply state the result as :

THEOREM 4. *The discriminant of minimum absolute value of quintic fields with three real and two imaginary conjugate fields is* -4511, *the corresponding field being* $R(\rho)$, *where* ρ *is a root of the equation*

$$x^5 - 2x^3 + x^2 - 1 = 0.$$

It appears likely that the second minimum is -4903, the corresponding field being defined by $x^5 + x^4 - x^3 - 2x^2 - x + 1 = 0$. The succeeding minima appear to be -5519, -5783, -7031, -7367, -7463, -8519, -8647, -9439, -9759, -10407, ... The method gives an even more extensive table of fields and discriminants in this case.

These results were contained in a dissertation accepted in 1953 for the Ph.D. degree by the University of Cambridge. H. Cohn [2] has recently predicted the results in a numerical study of certain quintics.

REFERENCES

1. W. E. H. Berwick, *Integral bases*, Cambridge Tracts on Mathematics (no. 22) (Cambridge, 1927).

2. H. Cohn, A numerical study of quintics of small discriminant, *Comm. Pure Appl. Math.* **8** (1955), 377–386.

3. G. H. Hardy, J. E. Littlewood, G. Polya, *Inequalities* (Cambridge, 1934), 52.

4. K. Hensel, *Theorie der algebraischen Zahlen* (Leipzig und Berlin, 1908), (*a*) 117, (*b*) 226, 231.

5. C. Hermite, Sur l'équation du cinquième degré, *C. R. Acad. Sci. Paris*, **62** (1866), (*a*) 67, (*b*) 71.

6. J. Mayer, Die absolut-kleinsten Diskriminanten der biquadratischen Zahlkörper, *S.-B. Akad. Wiss. Wien* Abt. IIa. **138** (1929), 733–742.

THE UNIVERSITY
GLASGOW