ACTA ARITHMETICA
XXXIV (1977)

Equations with equivalent roots

by

J. H. E. Cohn (London)

The quadratic equation $2x^2+x-7=0$ has two real roots $\frac{1}{4}(-1\pm\sqrt{57})$ whose representations as continued fractions are respectively

$$[1,\overline{1,1,1,3,7,3}] \quad \text{and} \quad [-3,1,6,3,\overline{1,1,1,3,7,3}].$$

Such numbers, which have the same elements in their continued fractions from some point onwards, are called *equivalent*. Writing down some quadratic equations with real roots at random, it will be found that this phenomenon occurs surprisingly often, although not always. It is the object of this note to discuss under what circumstances this happens for quadratic and higher degree equations. Throughout we assume that all the equations are irreducible over Z, the ring of rational integers.

We observe that two real numbers θ and ψ are equivalent in the above sense if and only if

$$\psi=\frac{A\theta+B}{C\theta+D}$$

where $A, B, C, D\in Z$ and $AD-BC=\pm1$, i.e., if and only if $\psi=\tau\theta$ where τ is a unimodular transformation. We recall that the unimodular transformations form a group Γ under composition and that τ may be represented by the matrix $T=\begin{pmatrix}A & B\\ C & D\end{pmatrix}$; then $\tau_1\tau_2$ is represented by the matrix T_1T_2 and the matrices T and $-T$ are identified in the sense that they correspond to the same τ.

Regarded as a transformation over the complex plane $\tau: C\to C$ is 1-1 and onto, with the usual convention regarding ∞, and unless τ is the identity transformation ι, τ has at most two distinct fixed points; these will be either rational or quadratic algebraic numbers.

The two following lemmas are well-known and easily proved.

Lemma 1. *The group Γ has precisely the following elements of finite order, viz.,*

(a) *the identity* ι,

(b) *elements of order* 2, *satisfying* $A+D=0$,

(c) *elements of order* 3, *satisfying* $A+D=\pm1$, $AD-BC=1$.

LEMMA 2. *The only finite subgroups of* Γ *have order* 1, 2, 3, 4 *or* 6.

THEOREM 1. *The roots of* $ax^2+bx+c=0$ *are equivalent if and only if the quadratic form* $a^2X^2+(b^2-2ac)XY+c^2Y^2$ *represents at least one of* b^2 *and* $-b^2$.

Proof. The roots are

$$\theta = -\frac{b+d^{1/2}}{2a} \quad \text{and} \quad \psi = -\frac{b-d^{1/2}}{2a} \quad \text{where} \quad d = b^2-4ac.$$

If $\psi = (A\theta+B)/(C\theta+D)$ with $AD-BC = \pm 1$, then $Cc/a+D\psi = A\theta+B$ i.e., $Cc/a+D(\theta+\psi) = (A+D)\theta+B$, i.e., $Cc-Db = a(A+D)\theta+aB$.

Now θ is irrational and so we have $A+D=0$, whence $A^2+BC = \mp 1$, $Cc+Ab = aB$. Thus $\mp b^2 = b^2BC+(Cc-aB)^2 = a^2B^2+(b^2-2ac)BC+c^2C^2$, as required.

Conversely if $\mp b^2 = a^2X^2+(b^2-2ac)XY+c^2Y^2$, then $b^2 \mid (aX-cY)^2$, say $aX-cY = bZ$. Then $Z^2+XY = \mp 1$ and $X-\theta\psi Y = -(\theta+\psi)Z$, i.e., $\psi = (\theta Z+X)/(\theta Y-Z)$ and so θ and ψ are equivalent.

The condition in the theorem is certainly satisfied if $a = c$ or $-c$, for then take $X=1$, $a-cY=0$; also if $a \mid b$ for then take $X = b/a$, $Y=0$; similarly if $c \mid b$. However suppose $a=2$, $b=1$, $c=-\lambda$ with $\lambda > 0$. Then we require $4X^2+(4\lambda+1)XY+\lambda^2Y^2 = \pm 1$ and so Y must be odd. Thus we find that $(8X+(4\lambda+1)Y)^2-(8\lambda+1)Y^2 = \pm 16$, and so $Z^2-(8\lambda+1)Y^2 = \pm 16$ must have a solution with Y and Z both odd. But then $(Y,Z)=1$ and at least if λ is sufficiently large Z/Y must be a convergent to the continued fraction for $(8\lambda+1)^{1/2}$. But if $8\lambda = n^2$, the continued fraction for $(8\lambda+1)^{1/2} = (n^2+1)^{1/2} = [n, \overline{2n}]$ and the convergents p/q all satisfy $p^2-(n^2+1)q^2 = \pm 1$. Thus there can be no representation in the form required. The least λ for which $2x^2+x-\lambda = 0$ is irreducible and $Z^2-(8\lambda+1)Y^2 = \pm 16$ fails to have a solution with both Y and Z odd is $\lambda = 18$. In this case we find that the equation $2x^2+x-18 = 0$ has roots

$$\theta = \frac{-1+\sqrt{145}}{4} = [2, \overline{1, 3, 5}]$$

and

$$\psi = \frac{-1-\sqrt{145}}{4} = [-4, 1, 2, \overline{1, 5, 3}]$$

which are not equivalent.

Next consider an irreducible cubic equation

$$F(x) \equiv ax^3+bx^2+cx+d = 0$$

with $a, b, c, d \in Z$ and $(a, b, c, d) = 1$, having three real roots, two of which are equivalent. Then if θ and $\tau\theta = (A\theta+B)/(C\theta+D)$ are the

equivalent roots with $AD-BC = \pm 1$, define the polynomial

$$\tau F(x) \equiv a(Ax+B)^3+b(AX+B)^2(Cx+D)+c(Ax+B)(Cx+D)^2+d(Cx+D)^3.$$

Then $\tau F(\theta) = (C\theta+D)^3 F(\tau\theta) = 0$ and so τF has θ as a root. Since F is irreducible, $\tau F = kF$ for some constant k. Since

$$\tau F(0) = aB^3+bB^2D+cBD^2+dD^3 \neq 0$$

as B, D cannot both be zero, $k \neq 0$. It follows that for any root α of F,

$$0 = kF(\alpha) = \tau F(\alpha) = (C\alpha+D)^3 F(\tau\alpha)$$

and so $\tau\alpha$ is also a root. Hence $\theta, \tau\theta, \tau^2\theta, \tau^3\theta, \ldots$ are all roots of F and since there are precisely three roots in all these cannot all be distinct.

Now since F is irreducible, no root of F can be a fixed point of any unimodular transformation apart from the identity. Now $\tau \neq \iota$ and $\tau^2 \neq \iota$ otherwise the roots of F would be θ, $\tau\theta$ and α, say. Now $\tau\alpha$ is also a root; but $\tau\alpha \neq \alpha$ since α is not a fixed point of τ, $\tau\alpha \neq \tau\theta$ since $\alpha \neq \theta$ and $\tau\alpha \neq \theta$ since otherwise $\alpha = \tau^2\alpha = \tau\theta$. Thus $\tau^3 = \iota$ and so the roots of F must be $\theta, \tau\theta, \tau^2\theta$, i.e., all be equivalent.

It then follows that the roots are

$$\theta, \ \frac{A\theta+B}{C\theta+D}, \ \frac{-D\theta+B}{C\theta-A}$$

and so the field $Q(\theta)$ is cyclic. Thus we have

THEOREM 2. *A necessary condition for a cubic equation to have two equivalent roots is that the discriminant be a perfect square.*

In the opposite direction suppose $F(x) = 0$ is an irreducible cubic equation whose discriminant is a perfect square. Then if θ is a root, the field $Q(\theta)$ is cyclic and so the other two roots lie in the field. If α is one such then $\alpha = k_1+k_2\theta+k_3\theta^2$ where $k_1, k_2, k_3 \in Q$ and we find easily that $\alpha = (A\theta+B)/(C\theta+D)$ where $A, B, C, D \in Z$ and $AD-BC \neq 0$. It is not necessarily the case that $AD-BC = 1$; for example if $F(x) \equiv x^3-3x^2-24x-1$, with discriminant 3^{10}, we find that the roots are

$$\theta, \ \frac{\theta-7}{\theta+2}, \ \frac{2\theta+7}{1-\theta}$$

which are not equivalent.

Let $z^* = (Az+B)/(Cz+D)$ for each complex z. Then since $\alpha = \theta^*$ is a root of $F(x) = 0$, we have

$$a(Ax+B)^3+b(Ax+B)^2(Cx+D)+c(Ax+B)(Cx+D)^2+d(Cx+D)^3 \equiv kF(x)$$

and so $\theta, \theta^*, \theta^{**}, \theta^{***}, \ldots$ are all roots of $F(x) = 0$. Thus as before $\theta = \theta^{***}$. We find easily that this requires simultaneously $BL = CL = (A-D)L = 0$, where $L = A^2+AD+D^2+BC$. Since $\theta \neq \theta^*$ we cannot have $B = C = (A-D) = 0$ and so $L = 0$. Thus $(A+D)^2 = AD-BC$ and so $AD-BC$ must be a perfect square.

We now show that although $F(x) = 0$ need not have equivalent roots, for suitably chosen integers l, m, n the equation with roots $(l\theta+m)/n$ etc., which also has square discriminant and which generates the same field $Q(\theta)$, does have equivalent roots. For suppose as above that

$$\theta^* = \frac{A\theta+B}{C\theta+D}$$

with $(A+D)^2 = AD-BC \neq 1$; without loss of generality suppose $(A, B, C, D) = 1$. If $(A, D) \neq 1$ let p be a prime dividing (A, D). Then $BC = AD-(A+D)^2 \equiv 0 \pmod{p^2}$. Since $(A, B, C, D) = 1$ we must have $p^2 \mid B$ or $p^2 \mid C$. If $p^2 \mid B$ then

$$\frac{\theta^*}{p} = \frac{\frac{A}{p}\left(\frac{\theta}{p}\right)+\frac{B}{p^2}}{C\left(\frac{\theta}{p}\right)+\frac{D}{p}} = \frac{A_1\left(\frac{\theta}{p}\right)+B_1}{C_1\left(\frac{\theta}{p}\right)+D_1}, \text{ say.}$$

Thus the equation with roots θ/p etc., has

$$A_1D_1-B_1C_1 = \frac{AD-BC}{p^2} < AD-BC.$$

Similarly if $p^3 \mid C$ then

$$p\theta^* = \frac{\frac{A}{p}(p\theta)+B}{\frac{C}{p^2}(p\theta)+\frac{D}{p}}.$$

Continuing in like fashion we reach a stage at which $(A, D) = 1$. If now $AD-BC \neq 1$, let p denote a prime dividing $AD-BC$; then $p \mid (A+D)$ and since $(A, D) = 1$, $p \nmid A$, $p \nmid D$. Since $BC = AD-(A+D)^2 \equiv AD \pmod{p}$, $p \nmid BC$. Now for any integer k,

$$\theta^*+k = k+\frac{A\theta+B}{C\theta+D} = \frac{(A+Ck)(\theta+k)+(B+kD-kA-k^2C)}{C(\theta+k)+(D-Ck)}$$
$$= \frac{A_1(\theta+k)+B_1}{C_1(\theta+k)+D_1}, \text{ say.}$$

Then $(A_1+D_1)^2 = (A+D)^2 = AD-BC = A_1D_1-B_1C_1$. But now $p \nmid A$, $p \nmid C$ and so choosing k such that $p \mid A+Ck$, i.e., $p \mid A_1$ we find that $p \mid D_1$. Thus the previous method can be applied to reduce $AD-BC$ until finally we reach the stage at which $AD-BC = 1$.

For the example above, with $\theta^* = (\theta-7)/(\theta+2)$ we find that

$$\frac{\theta^*-1}{3} = \frac{-1}{\left(\frac{\theta-1}{3}\right)+1}$$

and so the equation $G(x) \equiv x^3-3x-1 = 0$ with roots $(\theta-1)/3$ etc., has the required property.

We now consider equations of higher degree. Let $F(x) \equiv \sum_{r=0}^{n} a_{n-r}x^r$ be an irreducible polynomial of degree n, i.e., $a_0 \neq 0$, with integer coefficients. If the equation $F(x) = 0$ has two equivalent roots θ and $\tau\theta = (A\theta+B)/(C\theta+D)$ with $AD-BC = \pm 1$ then as before

$$\tau F(x) \equiv \sum_{r=0}^{n} a_{n-r}(Ax+B)^r(Cx+D)^{n-r} \equiv kF(x)$$

for some non-zero constant k. Thus $\tau\alpha$ is a root of $F(x) = 0$ whenever α is a root. It follows that τ is of finite order since otherwise $\theta, \tau\theta, \tau^2\theta, \ldots$ are all distinct. It follows by Lemma 1 that τ has order 2 or 3. It then follows that all the roots of $F(x) = 0$ form pairs or triples of equivalent roots. Thus we have

THEOREM 3. *If the irreducible equation* $F(x) \equiv \sum_{r=0}^{n} a_{n-r}x^r = 0$ *with* $a_0 \neq 0$ *has equivalent roots* θ *and* $\tau\theta$ *then either* (1) $\tau^2 = \iota$, $2 \mid n$ *and the roots of* $F(x) = 0$ *form* $\frac{1}{2}n$ *pairs* $\alpha, \tau\alpha$ *of equivalent roots; or* (2) $\tau^3 = \iota$, $3 \mid n$ *and the roots of* $F(x) = 0$ *form* $\frac{1}{3}n$ *triples* $\alpha, \tau\alpha, \tau^2\alpha$ *of equivalent roots.*

Of possibly greater interest is the case in which *all* the roots are equivalent. In this case we must have a group of n unimodular transformations which transform any one root θ_1 respectively into $\theta_1, \theta_2, \ldots, \theta_n$. In view of Lemma 2 we obtain

THEOREM 4. *If the irreducible equation* $F(x) \equiv \sum_{r=0}^{n} a_{n-r}x^r = 0$ *with* $a_0 \neq 0$ *has all its roots equivalent then* $n = 2, 3, 4$ *or* 6.

That the cases $n = 4, 6$ can actually occur can be seen from the equations

$$x^4-10x^2+1 = 0$$

with roots $\theta = \sqrt{3}-\sqrt{2}$, $-\theta$, $1/\theta$ and $-1/\theta$ and

$$x^6-3x^5-3x^4+11x^3-3x^2-3x+1 = 0$$

with roots $\theta = 1.53208889\ldots$, $\theta^{-1}, 1-\theta, 1-\theta^{-1}, (1-\theta)^{-1}, \theta(\theta-1)^{-1}$.

ROYAL HOLLOWAY COLLEGE
Egham, Surrey, TW20 0EX

Received on 8. 4. 1976
and in revised form on 29. 6. 1976 (833)