III APPLICATIONS

by

A. N. Milgram

A. Solvable Groups.

Before proceeding with the applications we must discuss certain questions in the theory of groups. We shall assume several simple propositions: (a) If N is a normal subgroup of the group G, then the mapping $f(x) = xN$ is a homomorphism of G on the factor group G/N. f is called the natural homomorphism. (b) The image and the inverse image of a normal subgroup under a homomorphism is a normal subgroup. (c) If f is a homomorphism of the group G on G', then setting $N' = f(N)$, and defining the mapping g as $g(xN) = f(x)N'$, we readily see that g is a homomorphism of the factor group G/N on the factor group G'/N'. Indeed, if N is the inverse image of N' then g is an isomorphism.

We now prove

<u>THEOREM 1.</u> <u>(Zassenhaus)</u> <u>If U and V are subgroups of G, u and v normal subgroups of U and V, respectively, then the following three factor groups are isomorphic:</u> $u(U \cap V)/u(U \cap v)$, $v(U \cap V)/v(u \cap V)$, $(U \cap V)/(u \cap V)(v \cap U)$.

It is obvious that $U \cap v$ is a normal subgroup of $U \cap V$. Let f be the natural mapping of U on U/u. Call $f(U \cap V) = H$ and $f(U \cap v) = K$. Then $f^{-1}(H) = u(U \cap V)$ and $f^{-1}(K) = u(U \cap v)$ from which it follows that $u(U \cap V)/u(U \cap v)$ is isomorphic to H/K. If, however, we view f as defined only over $U \cap V$, then $f^{-1}(K) = [u \cap (U \cap V)]\ (U \cap v) = (u \cap V)(U \cap v)$ so that $(U \cap V)/(u \cap V)(U \cap v)$ is also isomorphic to H/K. Thus the first and third of the above factor groups are isomorphic to each other. Similarly, the second and third factor groups are isomorphic.

Corollary 1. If H is a subgroup and N a normal subgroup of the group G, then $H/H \cap N$ is isomorphic to HN/N, a subgroup of G/N.

Proof: Set $G = U$, $N = u$, $H = V$ and the identity $1 = v$ in Theorem 1.

Corollary 2. Under the conditions of Corollary 1, if G/N is abelian, so also is $H/H \cap N$.

Let us call a group G solvable if it contains a sequence of subgroups $G = G_0 \supset G_1 \supset \dots \supset G_s = 1$, each a normal subgroup of the preceding, and with G_{i-1}/G_i abelian.

THEOREM 2. Any subgroup of a solvable group is solvable.

For let H be a subgroup of G, and call $H_i = H \cap G_i$. Then that H_{i-1}/H_i is abelian follows from Corollary 2 above, where G_{i-1}, G_i and H_{i-1} play the role of G, N and H.

THEOREM 3. The homomorph of a solvable group is solvable.

Let $f(G) = G'$, and define $G_i' = f(G_i)$ where G_i belongs to a sequence exhibiting the solvability of G. Then by (c) there exists a homomorphism mapping G_{i-1}/G_i on G'_{i-1}/G_i'. But the homomorphic image of an abelian group is abelian so that the groups G_i' exhibit the solvability of G'.

B. Permutation Groups.

Any one to one mapping of a set of n objects on itself is called a permutation. The iteration of two such mappings is called their product. It may be readily verified that the set of all such mappings forms a group in which the unit is the identity map. The group is called the symmetric group on n letters.

Let us for simplicity denote the set of n objects by the numbers $1, 2, \ldots, n$. The mapping S such that $S(i) \equiv i+1 \bmod n$ will be denoted by $(123\ldots n)$ and more generally $(ij\ldots m)$ will denote the mapping T such that $T(i) = j, \ldots, T(m) = i$. If $(ij\ldots m)$ has k numbers, then it will be called a k cycle. It is clear that if $T = (ij\ldots s)$ then $T^{-1} = (s\ldots ji)$.

We now establish the

<u>Lemma.</u> <u>If a subgroup U of the symmetric group on n letters ($n > 4$) contains every 3-cycle, and if u is a normal subgroup of U such that U/u is abelian, then u contains every 3-cycle.</u>

Proof: Let f be the natural homomorphism $f(U) = U/u$ and let $x = (ijk)$, $y = (krs)$ be two elements of U, where i, j, k, r, s are 5 numbers. Then, since U/u is abelian, setting $f(x) = x'$, $f(y) = y'$ we have $f(x^{-1}y^{-1}xy) = x'^{-1}y'^{-1}x'y' = 1$, so that $x^{-1}y^{-1}xy \in u$. But $x^{-1}y^{-1}xy = (kji)\cdot(srk)\cdot(ijk)\cdot(krs) = (kjs)$ and for each k, j, s we have $(kjs) \in u$.

<u>THEOREM 4.</u> <u>The symmetric group G on n letters is not solvable for $n > 4$.</u>

If there were a sequence exhibiting the solvability, since G contains every 3-cycle, so would each succeeding group, and the sequence could not end with the unit.

C. <u>Solution of Equations by Radicals.</u>

The extension field E over F is called an <u>extension by radicals</u> if there exist intermediate fields $B_1, B_2, \ldots, B_r = E$ and $B_i = B_{i-1}(\alpha_i)$ where each α_i is a root of an equation of the form $x^{n_i} - a_i = 0$, $a_i \in B_{i-1}$. A polynomial $f(x)$ in a field F is said to be <u>solvable by radicals</u> if its splitting field lies in an extension by radicals. We assume unless otherwise specified that the base field has characteristic 0 and that F contains as many roots of unity as are needed to make our subsequent statements valid.

Let us remark first that any extension of F by radicals can always be extended to an extension of F by radicals which is normal over F. Indeed B_1 is a normal extension of B_o since it contains not only α_1, but $\varepsilon\alpha_1$, where ε is any n_1-root of unity, so that B_1 is the splitting field of $x^{n_1} - a_1$. If $f_1(x) = \prod_\sigma(x^{n_2} - \sigma(a_2))$, where σ takes all values in the group of automorphisms of B_1 over B_o, then f_1 is in B_o, and adjoining successively the roots of $x^{n_2} - \sigma(a_2)$ brings us to an extension of B_2 which is normal over F. Continuing in this way we arrive at an extension of E by radicals which will be normal over F. We now prove the

<u>THEOREM 5.</u> <u>The polynomial f(x) is solvable by radicals if and only if its group is solvable.</u>

Suppose f(x) is solvable by radicals. Let E be a normal extension of F by radicals containing the splitting field B of f(x), and call G the group of E over F. Since for each i B_i is a Kummer extension of B_{i-1}, the group of B_i over B_{i-1} is abelian. In the sequence of groups $G = G_{B_o} \supset G_{B_1} \supset \ldots \supset G_{B_r} = 1$ each is a normal subgroup of the preceding since $G_{B_{i-1}}$ is the group of E over B_{i-1} and B_i is a normal extension of B_{i-1}. But $G_{B_{i-1}}/G_{B_i}$ is the group of B_i over B_{i-1} and hence is abelian. Thus G is solvable. However, G_B is a normal subgroup of G, and G/G_B is the group of B over F, and is therefore the group of the polynomial $f(x)$. But G/G_B is a homomorph of the solvable group G and hence is itself solvable.

On the other hand, suppose the group G of $f(x)$ to be solvable and let E be the splitting field. Let $G = G_0 \supset G_1 \supset \dots \supset G_r = 1$ be a sequence with abelian factor groups. Call B_i the fixed field for G_i. Since G_{i-1} is the group of E over B_{i-1} and G_i is a normal subgroup of G_{i-1}, then B_i is normal over B_{i-1} and the group G_{i-1}/G_i is abelian. Thus B_i is a Kummer extension of B_{i-1}, hence is splitting field of a polynomial of the form $(x^n-a_1)(x^n-a_2)\dots(x^n-a_s)$ so that by forming the successive splitting fields of the x^n-a_k we see that B_i is an extension of B_{i-1} by radicals, from which it follows that E is an extension by radicals.

Remark. The assumption that F contains roots of unity is not necessary in the above theorem. For if $f(x)$ has a solvable group G, then we may adjoin to F a primitive n^{th} root of unity, where n is, say, equal to the order of G. The group of $f(x)$ when considered as lying in F' is, by the theorem of Natural Rationality, a subgroup G' of G, and hence is solvable. Thus the splitting field over F' of $f(x)$ can be obtained by radicals. Conversely, if the splitting field E over F of $f(x)$ can be obtained by radicals, then by adjoining a suitable root of unity E is extended to E' which is still normal over F. But E' could be obtained by adjoining first the root of unity, and then the radicals, to F; F would first be extended to F' and then F' would be extended to E'. Calling G the group of E' over F and G' the group of E' over F', we see that G' is solvable and G/G' is the group of F' over F and hence abelian. Thus G is solvable. The factor group G/G_E is the group of $f(x)$ and being a homomorph of a solvable group is also solvable.

D. The General Equation of Degree n.

If F is a field, the collection of rational expressions in the variables $u_1, u_2, \ldots, u_n$ with coefficients in F is a field $F(u_1, u_2, \ldots, u_n)$. By the general equation of degree n we mean the equation

$$(1) \qquad f(x) = x^n - u_1 x^{n-1} + u_2 x^{n-2} - + \ldots + (-1)^n u_n.$$

Let E be the splitting field of $f(x)$ over $F(u_1, u_2, \ldots, u_n)$. If $v_1, v_2, \ldots, v_n$ are the roots of $f(x)$ in E, then $u_1 = v_1 + v_2 + \ldots + v_n$, $u_2 = v_1 v_2 + v_1 v_3 + \ldots + v_{n-1} v_n, \ldots$ $\ldots, u_n = v_1 \cdot v_2 \cdot \ldots \cdot v_n$.

We shall prove that the group of E over $F(u_1, u_2, \ldots, u_n)$ is the symmetric group.

Let $F(x_1, x_2, \ldots, x_n)$ be the field generated from F by the variables $x_1, x_2, \ldots, x_n$. Let $\alpha_1 = x_1 + x_2 + \ldots + x_n$, $\alpha_2 = x_1 x_2 + x_1 x_3 + \ldots + x_{n-1} x_n, \ldots, \alpha_n = x_1 x_2 \ldots x_n$ be the elementary symmetric functions, i.e., $(x - x_1)(x - x_2) \ldots (x - x_n) = x^n - \alpha_1 x^{n-1} + - \ldots (-1)^n \alpha_n = f^*(x)$. If $g(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a polynomial in $\alpha_1, \ldots, \alpha_n$, then $g(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ only if g is the zero polynomial. For if $g(\Sigma x_i, \Sigma x_i x_k, \ldots) = 0$, then this relation would hold also if the x_i were replaced by the v_i. Thus, $g(\Sigma v_i, \Sigma v_i v_k, \ldots) = 0$ or $g(u_1, u_2, \ldots, u_n) = 0$ from which it follows that g is identically zero.

Between the subfield $F(\alpha_1,\ldots,\alpha_n)$ of $F(x_1,\ldots,x_n)$ and $F(u_1,u_2,\ldots,u_n)$ we set up the following correspondence: Let $f(u_1,\ldots,u_n)/g(u_1,\ldots,u_n)$ be an element of $F(u_1,\ldots,u_n)$. We make this correspond to $f(\alpha_1,\ldots,\alpha_n)/g(\alpha_1,\ldots,\alpha_n)$. This is clearly a mapping of $F(u_1,u_2,\ldots,u_n)$ on all of $F(\alpha_1,\ldots,\alpha_n)$. Moreover, if $f(\alpha_1,\alpha_2,\ldots,\alpha_n)/g(\alpha_1,\alpha_2,\ldots,\alpha_n) =$ $f_1(\alpha_1,\alpha_2,\ldots,\alpha_n)/g_1(\alpha_1,\alpha_2,\ldots,\alpha_n)$, then $fg_1 - gf_1 = 0$. But this implies by the above that

$f(u_1,\ldots,u_n)\cdot g_1(u_1,\ldots,u_n) - g(u_1,\ldots,u_n)\cdot f_1(u_1,\ldots,u_n) = 0$

so that $f(u_1,\ldots,u_n)/g(u_1,u_2,\ldots,u_n) =$ $f_1(u_1,\ldots,u_n)/g_1(u_1,u_2,\ldots,u_n)$. It follows readily from this that the mapping of $F(u_1,u_2,\ldots,u_n)$ on $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ is an isomorphism. But under this correspondence $f(x)$ corresponds to $f^*(x)$. Since E and $F(x_1,x_2,\ldots,x_n)$ are respectively splitting fields of $f(x)$ and $f^*(x)$, by Theorem 10 the isomorphism can be extended to an isomorphism between E and $F(x_1,x_2,\ldots,x_n)$. Therefore, the group of E over $F(u_1,u_2,\ldots,u_n)$ is isomorphic to the group of $F(x_1,x_2,\ldots,x_n)$ over $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Each permutation of $x_1,x_2,\ldots,x_n$ leaves $\alpha_1,\alpha_2,\ldots,\alpha_n$ fixed and, therefore, induces an automorphism of $F(x_1,x_2,\ldots,x_n)$ which leaves $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ fixed. Conversely, each automorphism of $F(x_1,x_2,\ldots,x_n)$ which leaves $F(\alpha_1,\ldots,\alpha_n)$ fixed must permute the roots $x_1,x_2,\ldots,x_n$ of $f^*(x)$ and is completely determined by the permutation it effects on $x_1,x_2,\ldots,x_n$. Thus, the group of $F(x_1,x_2,\ldots,x_n)$ over $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ is the symmetric group on n letters. Because of the isomorphism between $F(x_1,\ldots,x_n)$ and E, the group for E over $F(u_1,u_2,\ldots,u_n)$ is also the symmetric group. If we remark that the symmetric group for $n > 4$ is not solvable, we obtain from the theorem on solvability of equations the famous theorem of Abel:

THEOREM 6. The group of the general equation of degree n is the symmetric group on n letters. The general equation of degree n is not solvable by radicals if $n > 4$.

E. Solvable Equations of Prime Degree.

The group of an equation can always be considered as a permutation group. If $f(x)$ is a polynomial in a field F, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(x)$ in the splitting field $E = F(\alpha_1, \ldots, \alpha_n)$. Then each automorphism of E over F maps each root of $f(x)$ into a root of $f(x)$, that is, permutes the roots. Since E is generated by the roots of $f(x)$, different automorphisms must effect distinct permutations. Thus, the group of E over F is a permutation group acting on the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $f(x)$.

For an irreducible equation this group is always transitive. For let α and α' be any two roots of $f(x)$, where $f(x)$ is assumed irreducible. $F(\alpha)$ and $F(\alpha')$ are isomorphic where the isomorphism is the identity on F, and this isomorphism can be extended to an automorphism of E (Theorem 10). Thus, there is an automorphism sending any given root into any other root, which establishes the "transitivity" of the group.

A permutation σ of the numbers $1, 2, \ldots, q$ is called a linear substitution modulo q if there exists a number $b \not\equiv 0$ modulo q such that $\sigma(i) \equiv bi + c \pmod{q}$, $i = 1, 2, \ldots, q$.

THEOREM 7. Let $f(x)$ be an irreducible equation of prime degree q in a field F. The group G of $f(x)$ (which is a permutation group of the roots, or the numbers $1, 2, \ldots, q$) is solvable

<u>if and only if, after a suitable change in the numbering of the roots, G is a group of linear substitutions modulo q, and in the group G all the substitutions with b = 1, $\sigma(i) \equiv c + i$ (c = 1,2,...,q) occur.</u>

Let G be a transitive substitution group on the numbers 1,2,...,q and let G_1 be a normal subgroup of G. Let 1,2,...,k be the images of 1 under the permutations of G_1; we say: 1,2,...,k is a <u>domain of transitivity</u> of G_1. If $i \leq q$ is a number not belonging to this domain of transitivity, there is a $\sigma \varepsilon G$ which maps 1 on i. Then $\sigma(1,2,\ldots,k)$ is a domain of transitivity of $\sigma G_1 \sigma^{-1}$. Since G_1 is a normal subgroup of G, we have $G_1 = \sigma G_1 \sigma^{-1}$. Thus, $\sigma(1,2,\ldots,k)$ is again a domain of transitivity of G_1 which contains the integer i and has k elements. Since i was arbitrary, the domains of transitivity of G_1 all contain k elements. Thus, the numbers 1,2,...,q are divided into a collection of mutually exclusive sets, each containing k elements, so that k is a divisor of q. Thus, in case q is a prime, either k = 1 (and then G_1 consists of the unit alone) or k = q and G_1 is also transitive.

To prove the theorem, we consider the case in which G is solvable. Let $G = G_0 \supset G_1 \supset \ldots \supset G_{s+1} = 1$ be a sequence exhibiting the solvability. Since G_s is abelian, choosing a cyclic subgroup of it would permit us to assume the term before the last to be cyclic, i.e., G_s is cyclic. If σ is a generator of G_s, σ must consist of a cycle containing all q of the numbers 1,2,...,q since in any other case G_s would not be transitive [if $\sigma = (1ij\ldots m)(n\ldots p)\ldots$ then the powers of σ would map 1 only into 1,i,j...m, contradicting the transitivity of G_s]. By a change in the numbering of the permutation letters, we may assume

$$\sigma(i) \equiv i + 1 \pmod q ,$$

$$\sigma^c(i) \equiv i + c \pmod q .$$

Now let τ be any element of G_{s-1}. Since G_s is a normal subgroup of G_{s-1}, $\tau\sigma\tau^{-1}$ is an element of G_s, say $\tau\sigma\tau^{-1} = \sigma^b$. Let $\tau(i) = j$ or $\tau^{-1}(j) = i$, then
$\tau\sigma\tau^{-1}(j) = \sigma^b(j) \equiv j + b \pmod q$. Therefore,
$\tau\sigma(i) \equiv \tau(i) + b \pmod q$ or $\tau(i+1) \equiv \tau(i) + b$ for each i.
Thus, setting $\tau(o) = c$, we have $\tau(1) \equiv c + b$,
$\tau(2) \equiv \tau(1) + b = c + 2b$ and in general $\tau(i) \equiv c + ib \pmod q$.
Thus, each substitution in G_{s-1} is a linear substitution. Moreover, the only elements of G_{s-1} which leave no element fixed belong to G_s, since for each $a \not\equiv 1$, there is an i such that $ai + b \equiv i \pmod q$ [take i such that $(a-1)i \equiv -b$].

We prove by an induction that the elements of G are all linear substitutions, and that the only cycles of q letters belong to G_s. Suppose the assertion true of G_{s-n}. Let $\tau \varepsilon G_{s-n-1}$ and let σ be a cycle which belongs to G_s (hence also to G_{s-n}). Since the transform of a cycle is a cycle, $\tau^{-1}\sigma\tau$ is a cycle in G_{s-n} and hence belongs to G_s. Thus $\tau^{-1}\sigma\tau = \sigma^b$ for some b. By the argument in the preceding paragraph, τ is a linear substitution $bi + c$ and if τ itself does not belong to G_s, then τ leaves one integer fixed and hence is not a cycle of q elements.

We now prove the second half of the theorem. Suppose G is a group of linear substitutions which contains a subgroup N of the form $\sigma(i) \equiv i + c$. Since the only linear substitutions which do not leave an integer fixed belong to N, and since the transform of a cycle of q elements is again a cycle of q elements, N is a normal subgroup of G. In each coset $N \cdot \tau$ where $\tau(i) \equiv bi + c$ the substitution $\sigma^{-1}\tau$ occurs, where $\sigma \equiv i + c$. But $\sigma^{-1}\tau(i) \equiv (bi+c) - c = bi$. Moreover, if $\tau(i) \equiv bi$ and $\tau'(i) \equiv b'i$ then $\tau\tau'(i) \equiv bb'i$. Thus, the factor group (G/N) is isomorphic to a multiplicative subgroup of the numbers $1, 2, \ldots, q-1$ mod q and is therefore abelian. Since (G/N) and N are both abelian, G is solvable.

Corollary 1. If G is a solvable transitive substitution group on q letters (q prime), then the only substitution of G which leaves two or more letters fixed is the identity.

This follows from the fact that each substitution is linear modulo q and $bi + c \equiv i \pmod{q}$ has either no solution ($b \equiv 1$, $c \not\equiv 0$) or exactly solution ($b \not\equiv 1$) unless $b \equiv 1$, $c \equiv 0$ in which case the substitution is the identity.

Corollary 2. A solvable, irreducible equation of prime degree in a field which is a subset of the real numbers has either one real root or all its roots are real.

The group of the equation is a solvable transitive substitution group on q (prime) letters. In the splitting field (contained in the field of complex numbers) the automorphism which maps a number into its complex conjugate would leave fixed all the real numbers. By Corollary 1, if two roots are left fixed, then all the roots are left fixed, so that if the equation has two real roots all its roots are real.

F. Ruler and Compass Constructions.

Suppose there is given in the plane a finite number of elementary geometric figures, that is, points, straight lines and circles. We seek to construct others which satisfy certain conditions in terms of the given figures.

Permissible steps in the construction will entail the choice of an arbitrary point interior to a given region, drawing a line through two points and a circle with given center and radius, and finally intersecting pairs of lines, or circles, or a line and circle.

Since a straight line, or a line segment, or a circle is determined by two points, we can consider ruler and compass constructions as constructions of points from given points, subject to certain conditions.

If we are given two points we may join them by a line, erect a perpendicular to this line at, say, one of the points and, taking the distance between the two points to be the unit, we can with the compass lay off any integer n on each of the lines. Moreover, by the usual method, we can draw parallels and can construct m/n. Using the two lines as axes of a cartesian coordinate system, we can with ruler and compass construct all points with rational coordinates.

If a,b,c,... are numbers involved as coordinates of points which determine the figures given, then the sum, product, difference and quotient of any two of these numbers can be constructed. Thus, each element of the field $R(a,b,c,\ldots)$ which they generate out of the rational numbers can be constructed.

It is required that an arbitrary point is any point of a given region. If a construction by ruler and compass is possible, we can always choose our arbitrary points as points having rational coordinates. If we join two points with coefficients in $R(a,b,c,\ldots)$ by a line, its equation will have coefficients in $R(a,b,c,\ldots)$ and the intersection of two such lines will be a point with coordinates in $R(a,b,c,\ldots)$. The equation of a circle will have coefficients in the field if the circle passes through three points whose coordinates are in the field or if its center and one point have coordinates in the field. However, the coordinates of the intersection of two such circles, or a straight line and circle, will involve square roots.

It follows that if a point can be constructed with a ruler and compass, its coordinates must be obtainable from $R(a,b,c,\ldots)$ by a formula only involving square roots, that is, its coordinates will lie in a field $R_s \supset R_{s-1} \supset \ldots \supset R_1 = R(a,b,c,\ldots)$ where each field R_i is splitting field over R_{i-1} of a quadratic equation $x^2 - \alpha = 0$. It follows (Theorem 6, p. 13) since either $R_i = R_{i-1}$ or $(R_i/R_{i-1}) = 2$, that (R_s/R_1) is a power of two. If x is the coordinate of a constructed point, then $(R_1(x)/R_1)\cdot(R_s/R_1(x)) = (R_s/R_1) = 2^\nu$ so that $R_1(x)/R_1$ must also be a power of two.

Conversely, if the coordinates of a point can be obtained from $R(a,b,c,\ldots)$ by a formula involving square roots only, then the point can be constructed by ruler and compass.

For, the field operations of addition, subtraction, multiplication and division may be performed by ruler and compass constructions and, also, square roots using $1:r = r:r_1$ to obtain $r = \sqrt{r_1}$ may be performed by means of ruler and compass constructions.

As an illustration of these considerations, let us show that it is impossible to trisect an angle of 60°. Suppose we have drawn the unit circle with center at the vertex of the angle, and set up our coordinate system with X-axis as a side of the angle and origin at the vertex.

Trisection of the angle would be equivalent to the construction of the point ($\cos 20^\circ$, $\sin 20^\circ$) on the unit circle. From the equation $\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta$, the abscissa would satisfy $4x^3 - 3x = 1/2$. The reader may readily verify that this equation has no rational roots, and is therefore irreducible in the field of rational numbers. But since we may assume only a straight line and unit length given, and since the 60° angle can be constructed, we may take $R(a,b,c,\ldots)$ to be the field R of rational numbers. A root α of the irreducible equation $8x^3 - 6x - 1 = 0$ is such that $(R(\alpha)/R) = 3$, and not a power of two.