Suppose $f(z)$ is an irreducible polynomial of degree d over the field of rational numbers, and suppose that $f(z)$ has two roots α, β with α/β a primitive nth root of unity. Show that $\phi(n) \leqslant d$.

Solution by I. M. Isaacs, University of Wisconsin, Madison, WI. We are given $f(\alpha) = 0 = f(\beta)$ where f is irreducible over Q and $\alpha/\beta = \varepsilon$, a primitive nth root of unity. Let E be a splitting field for f containing α and β and let $G = \mathrm{Gal}(E/Q)$, the Galois group. Let $H = \mathrm{Gal}(E/Q(\alpha))$ and $K = \mathrm{Gal}(E/Q(\beta))$ and note that the subgroups H and K are conjugate in G since f is irreducible. Also

$$|G : H| = d = |G : K|,$$

where $d = \deg(f)$.

Now let $N = \mathrm{Gal}(E/Q(\varepsilon))$. Since ε is a root of unity, $Q(\varepsilon)$ is Galois over Q and so N is normal in G. Also, G/N is isomorphic to $\mathrm{Gal}(Q(\varepsilon)/Q)$ and so it is abelian of order $\phi(n)$. Now HN and KN are conjugate in G and since G/N is abelian, we conclude that $HN = KN \supseteq K$. We also have $H \cap K = H \cap N$, since an element of H fixes $\alpha = \beta\varepsilon$ and so it fixes β if and only if it fixes ε.

We have

$$|HN : H| \cdot |HN : K| \geqslant |HN : H \cap K| = |HN : H \cap N| = |HN : H| \cdot |H : H \cap N|,$$

and so $|HN : K| \geqslant |H : H \cap N| = |HN : N|$. We conclude that $|K| \leqslant |N|$ and so $d \geqslant \phi(n)$, as required.

Editorial Comment. Modifying the above argument by replacing group indices by the degrees of the corresponding field extensions leads to the following more general result, as was pointed out by Cantor. Let α and β be conjugate algebraic elements over a field k, and suppose K is an abelian extension of k contained in $k(\alpha, \beta)$; then $[K : k] \leqslant [k(\alpha) : k]$. A proof along these lines and a similar generalization was presented by Ze-Li Dou (student, Queens College, CUNY).

Many readers took questionable shortcuts here, and a number of proposed solutions were judged as either incorrect or incomplete.

Also solved by Ze-Li Dou, Edward H. Grossman, David R. Richman, John Henry Steelman, and the proposer.

An Alternating Sum of Products of Beta Random Variables

6524 [1986, 573]. *Proposed by Gérard Letac and Guy Yétèrian, Université Paul Sabatier, Toulouse, France.*

Let p and q be positive numbers, and $\{X_n\}_{n=0}^{\infty}$ a sequence of independent random variables with the same distribution

$$\beta_{p,q}(dx) = \frac{\Gamma(p+q)}{\Gamma(p)\Gamma(q)} x^{p-1}(1-x)^{q-1}\,dx$$

on $[0, 1]$. Find the distribution of

$$\sum_{n=0}^{\infty} (-1)^n X_0 X_1 \cdots X_n.$$

Solution by Western Maryland College Problems Group, Western Maryland College, Westminster. Let

$$Z_m = \sum_{n=0}^{m} (-1)^n X_0 X_1 \cdots X_n,$$

and set $Z = Z_\infty$. We will show that Z has a β density

$$g(t) = \frac{\Gamma(2p+q)}{\Gamma(p)\Gamma(p+q)} t^{p-1}(1-t)^{p+q-1} \text{ on } [0,1].$$

Observe that, since $P\{X_i \leqslant \frac{1}{2}\}$ is constant, the event $\{X_i \leqslant \frac{1}{2}\}$ occurs infinitely often (with probability one). Hence, the $(n+1)$-fold product of X_i contains a factor of an arbitrarily large power of $\frac{1}{2}$ if n is large enough; hence it converges to zero.

Now

$$P[X_n = 1 \text{ for some } n] \leqslant \sum_{n=0}^{\infty} P[X_n = 1] = 0.$$

Thus Z_m converges with probability one because the series is alternating and it fails to decrease with probability zero. It follows that Z_m converges in distribution to Z. Denote by G_m the distribution of Z_m and G the distribution of Z. We can factor out X_0 and write

$$Z_m = X_0\left[1 - \sum_{n=1}^{m} (-1)^{n-1} X_1 \cdots X_n\right] = X_0[1 - Y_{m-1}],$$

where Y_{m-1} is independent of X_0 and has the same distribution as Z_{m-1}. This will give us an integral equation satisfied by G. We write f for the density of X_0.

Now $G_m(t) = P[Z_m \leqq t]$ satisfies

$$\begin{aligned} G_m(t) &= P[X_0(1 - Y_{m-1}) \leqq t] \\ &= 1 - P[Y_{m-1} \leqq 1 - t/X_0] \\ &= 1 - \int_t^1 G_{m-1}(1 - t/s) f(s)\, ds. \end{aligned}$$

By letting m go to infinity we get

$$G(t) = 1 - \int_t^1 G(1 - t/s) f(s)\, ds.$$

This equation has a unique solution for $G \in L^1[0,1]$. To see this consider the operator ϕ defined by

$$\phi[H](t) = 1 - \int_t^1 H(1 - t/s) f(s)\, ds.$$

By a change in the order of integration, and the substitution $u = 1 - t/s$, we find that

$$\begin{aligned} \|\phi[H] - \phi[K]\| &= \left| \int_0^1 \int_t^1 (H(1 - t/s) - K(1 - t/s)) f(s)\, ds\, dt \right| \\ &\leqslant \int_0^1 \int_0^s |H(1 - t/s) - K(1 - t/s)| f(s)\, dt\, ds \\ &= \int_0^1 \int_0^1 |H(u) - K(u)| s f(s)\, du\, ds \\ &= \|H - K\| \mu, \end{aligned}$$

where $\mu = E[X_0] = p/(p+q) < 1$. By the contraction mapping theorem ϕ has a unique fixed point. Also, the equation for G shows that G has a continuous derivative on $(0,1)$. Upon differentiating the equation for G we get an equation satisfied by the density of Z, namely,

$$g(t) = \int_t^1 g(1 - t/s)s^{-1}f(s)\,ds.$$

This must also have a unique solution for g a probability density, because we can integrate to recover the equation for G and then differentiate to get g. It is now a relatively straightforward exercise in integral calculus to show (after some changes of variable) that the $g(t)$ mentioned at the start, i.e., the $\beta(p, p+q)$ density, satisfies this equation.

Editorial Comment. Specialists in probability theory might prefer a short proof given by Norman L. Johnson (University of North Carolina) who quickly obtains the result by taking rth moments of both sides of

$$Z_\infty = X_0(1 - Y_\infty), \qquad (*)$$

and by using the fact that the product of two mutually independent beta variables with parameters (p, q) and $(p+q, p)$ has a beta distribution with parameters $(p, p+q)$. O. P. Lossers (The Netherlands), whose solution is somewhat similar to the one from Western Maryland, also relies on moments to establish uniqueness. Lossers adds that the product relationship between (p, q), $(p+q, p)$ and $(p, p+q)$ is related to equalities for the order statistics $Y_{k;n}$ from the exponential distribution by

$$\exp(-Y_{k;n}) = X_{n-k,k}.$$

Here $X_{p,q}$ denotes a random variable with distribution $\beta_{p,q}$ and equality means equality in distribution.

The proposers note that for $p = q = 1$, the result is essentially due to T. Ugaheri, On a limit distribution, *Ann. Inst. Statist. Math. Tokyo*, 1 (1950) 157–160.

Also solved by Ignacy Icchak Kotlarski, Kenneth Schilling, Douglas P. Wiens, and the proposers.

A Matrix Whose Cube Is the Identity

6527 [1986, 659]. *Proposed by Nicholas Strauss, Boston University.*

Let $J(m)$ be the $m \times m$ matrix whose (i, j)th entry is

$$\binom{i+j}{j}, \quad 0 \leqslant i, j \leqslant m-1.$$

Show that for all primes p and positive integers n, the matrix $J(p^n)$ is a cube root of unity modulo p.

Solution by Ira Gessel, Brandeis University, Waltham, MA. Let $K(m)$ be the $m \times m$ matrix whose (i, j)th entry is

$$(-1)^j\binom{m-i-1}{j}, \qquad 0 \leqslant i, j \leqslant m-1.$$

Let Θ be the linear transformation on polynomials in x of degree less than m