AN ELEMENTARY PROOF OF KRONECKER'S THEOREM

JOEL SPENCER
Santa Monica, California 90406

Kronecker's Theorem. Let $p(x)$ be a monic polynomial with integral coefficients, irreducible over the integers, such that all roots α of p have $|\alpha| = 1$. Then all roots α are roots of unity.

This result was first proven by Kronecker using symmetric polynomials. In this note we prove Kronecker's Theorem using Linear Recursive Sequences. The condition that p is monic is necessary since $p(x) = 5x^2 - 6x + 5$ has roots $(3 \pm 4i)/5$. It is also necessary that *all* roots α have $|\alpha| = 1$. For let p be the minimal polynomial of $\alpha = x + i\sqrt{1 - x^2}$ where $x = \sqrt{2} - 1$. Then $|\alpha| = 1$ but $p(\beta) = 0$ where $\beta = y + i\sqrt{1 - y^2}$, $y = -\sqrt{2} - 1$ and $|\beta| > 1$.

Proof of Theorem. Let

$$p(x) = x^n - \sum_{i=1}^{n} a_i x^{n-i} .$$

Consider the sequence $\{u_i\}$ defined by

$$U_i = 0 \qquad [0 \leqslant i \leqslant n-2]$$

$$U_{n-1} = 1$$

(*)
$$U_s = \sum_{i=1}^{n} a_i U_{s-i} \quad \text{for } s \geqslant n$$

Then

$$U_s = \sum_{i=1}^{n} \xi_i \alpha_i^s ,$$

where $\alpha_1, \cdots, \alpha_n$ are the roots of p. Then

$$|U_s| \leqslant \sum_{i=1}^{n} |\xi_i|\,|\alpha_i|^s \leqslant \sum_{i=1}^{n} |\xi_i| \leqslant N ,$$

independent of s. Since the U_s are integers there are $\leqslant (2N + 1)$ possible U_s and hence $\leqslant (2N + 1)^n$ possible sequences $(U_s, U_{s+1}, \cdots, U_{s+(n-1)})$. Therefore, for some $0 \leqslant s \leqslant t \leqslant (2N + 1)^n + 1$,

$$(U_s, U_{s+1}, \cdots, U_{s+(n-1)}) = (U_t, U_{t+1}, \cdots, U_{t+(n-1)}).$$

That is

$$U_{s+j} = U_{t+j} \qquad (0 \leqslant j \leqslant n-1).$$

By (*) this implies

(**)
$$U_{s+j} = U_{t+j} \qquad (0 \leqslant j).$$

Setting $K = t - s$,

$$\sum_{i=1}^{n} \xi_i \alpha_i^{s+j} = \sum_{i=1}^{n} \xi_i \alpha_i^{s+j+k} \qquad (0 \leqslant j)$$

$$\sum_{i=1}^{n} [\xi_i(a_i^k - 1)]\, a_i^{s+j} = 0 \qquad (0 \leqslant j).$$

Setting $x_i = \xi_i(a_i^k - 1)$

$$\sum_{i=1}^{n} a_i^{s+j} x_i = 0 \qquad (0 \leqslant j \leqslant n-1).$$

The coefficient determinant

$$\det \begin{bmatrix} a_1^s & & a_n^s \\ a_1^{s+1} & & a_n^{s+1} \\ \vdots & \cdots & \vdots \\ a_1^{s+n-1} & & a_n^{s+n-1} \end{bmatrix} = (a_1 \cdots a_n)^s \det \begin{bmatrix} a_1^0 & & a_n^0 \\ a_1^1 & & a_n^1 \\ \vdots & \cdots & \vdots \\ a_1^{n-1} & & a_n^{n-1} \end{bmatrix} \neq 0,$$

since this is the Vandermonde matrix and the a_i are distinct since p is irreducible. Hence the n linear forms are independent, so

$$x_i = 0 \qquad (1 \leqslant i \leqslant n).$$

Some $\xi_i \neq 0$ since $U_{n-1} \neq 0$. For that i, $a_i^k = 1$. Since the a's are roots of an irreducible polynomial, by Galois theory $a_j^k = 1$ for $1 \leqslant j \leqslant n$.

Q.E.D.

Corollary. Kronecker's Theorem holds even if p is not irreducible.

Proof. We factor $p(x) = \Pi p_i(x)$, where the p_i are irreducible. All roots a of p_i are roots of p so $|a| = 1$ so all roots are roots of unity. But all roots of p are roots of some p_i and hence roots of unity.

David Cantor has noted that the proof after (**) can be shortened using generating functions. For

$$\sum_{i=0} U_i x^i = \frac{x^{n-1}}{1 - \sum_{i=1}^{n} a_i x^i} = \frac{A(x)}{x^k - 1}$$

Hence

$$x^n P(x^{-1}) = 1 - \sum_{i=1}^{n} a_i x^i \mid x^k - 1$$

$p(a) = 0$ implies $p(a^{-1}) = 0$ implies $a^{-k} - 1 = 0$, $a^{-k} = 1$, so $a^k = 1$.

****

[Continued from page 8.]

I must tell you that I am short of proofs and most of the propositions would have to be presented as observations or conjectures. Co-authors with proofs are welcome.

Thank you for your attention to this letter. Please write and let me know whether the subject is of interest, You are free, of course, to publish this letter or any part of it.

Sincerely,

John W. Jameson,
P. O. Box 205
Edgewood, Maryland 21040

****