The Mathematical Association

259, London Road,
Leicester,
LE2 3BE
United Kingdom
Telephone (0116) 221 0013
Fax (0116) 212 2835

Registered Charity No. 313281

The Mathematical Gazette
Editor: Gerry Leversha

15 Maunder Road,
Hanwell,
London
W7 3PN
United Kingdom
e-mail: g.leversha@btinternet.com

14-Dec-2012

Urgent - requires immediate attention

Dear

I enclose a proof copy of your contribution to the March 2013 issue of *The Mathematical Gazette*. It has already been checked once by our proof-readers, and some minor rewordings, punctuation changes, etc. may have been made. Please check it carefully for errors, paying special attention to the diagrams, mathematical expressions, quotations from other sources and your name and address. If you have any essential changes, please mark them clearly in the margin in a contrasting colour, indicating the place in the text where the alteration is to be made. **Whether or not you have made alterations, please return the proof copy to me.**

The copyright for all contributions to the March 2013 issue of *The Mathematical Gazette*, including the right to reproduce them in all forms and media, should be assigned exclusively to The Mathematical Association. Please complete the copyright transfer form below and return it with your proof copy. If your article contains copyright materials from previously published sources, including your own published work, you must obtain written permission from the copyright owner and send the letter granting this permission to me. The Mathematical Association grants *you* permission to reproduce *your* contribution for non-profit making scholarly or educational use. You must obtain written permission from the Editor in Chief of The Mathematical Association, at 259 London Road, Leicester LE2 3BE, if you wish to reproduce your contribution in any publication.

Time is of the essence at this stage of the publication process. If I have not heard from you by Friday 11th January 2013 I will have to assume that you accept the article as it stands and that you agree to the terms of publication described in the paragraph above. **In an emergency (only) you can fax the changes and reply form to Bill Richardson on 01343 860 450.**

Authors of articles, notes and matters for debate (*but not of letters, items in Feedback, or reviews*) may claim a free copy of the *Gazette.* All authors may claim an offprint of their contributions suitable for photocopying. If you wish to claim, please indicate on the form below.

Yours sincerely,

Gerry Leversha

I hereby assign the copyright for all my contributions to the March 2013 issue of *The Mathematical Gazette* to The Mathematical Association.

Signed : .... Telephone: ....

Address: ....

Title(s) of item(s) ....

Please send a complimentary copy of the March 2013 *Gazette* ☐ (tick)

Please send an offprint of my contribution(s) to the March 2013 *Gazette* ☐ pdf **or** ☐ paper

Composition of polynomials

B. SURY

Introduction

The motivation to write this paper arose out of the following problem which was posed in a recent mathematical olympiad:

> Given a polynomial $P(X)$ with integer coefficients, show that there exist non-zero polynomials $Q(X)$, $R(X)$ with integer coefficients such that $P(X)Q(X)$ is a polynomial in X^2 and $P(X)R(X)$ is a polynomial in X^3.

For instance, if $P(X) = 2 - 5X + 3X^2 + 12X^3$, then we notice that $Q(X) = 2 + 5X + 3X^2 - 12X^3$ serves the purpose for the first part, viz.,

$$P(X)Q(X) = \left(2 - 5X + 3X^2 + 12X^3\right)\left(2 + 5X + 3X^2 - 12X^3\right)$$

$$= \left(\left(2 + 3X^2\right) - \left(5X - 12X^3\right)\right)\left(\left(2 + 3X^2\right) + \left(5X - 12X^3\right)\right)$$

$$= \left(2 + 3X^2\right)^2 - \left(5X - 12X^3\right)^2 = \left(2 + 3X^2\right)^2 - X^2\left(5 - 12X^2\right)^2.$$

A moment's thought makes it fairly evident that this trick easily solves the first part of the problem for a *general* polynomial $P(X)$. For example, since $P(X)$ factorises over the complex numbers, we can write $P(X) = c\sum_{i=1}^{k}(X - \alpha_i)$, and choose $Q(X) = c\sum_{i=1}^{k}(X + \alpha_i)$ so that $P(X)Q(X) = c^2\prod_{i=1}^{n}(X^2 - \alpha_i^2)$. That both $Q(X)$ and $P(X)Q(X)$ have integer coefficients follows from the observation that $Q(X) = P(-X)$.*

What about the second part, or more generally, does the assertion hold good if we replace X^2, X^3 by any X^{k+1}? As a matter of fact, it turns out that we can retain the elementary level of the original problem and still give a proof for X^k which carries over to the general situation where X^k is replaced by an arbitrary, non-constant polynomial $f(X)$. At the end, we indicate a multi-variable generalisation which is at a slightly higher level of sophistication. We mention in passing that the decomposability of polynomials in one variable as a composition of polynomials of smaller degree, has come to be studied in depth in the past decade or so, in relation to solving Diophantine equations of the form $f(X) = g(Y)$ where f, g are integer polynomials in independent variables X, Y.

1. *The original problem for X^2, X^3*

Let us first solve the original problem. Given $P(X)$, consider the polynomial $Q(X) = P(-X)$. In other words, if $P(X) = a_0 + a_1X + \ldots + aX^n$, then

* Author, are the changes in this paragraph acceptable?

$$P(X) = (a_0 + a_2X^2 + \dots) + X(a_1 + a_3X^2 + \dots) = f(X^2) + Xg(X^2)$$

for certain polynomials $f,\ g$ with integer coefficients.

Taking $Q(X) = P(-X) = f(X^2) + Xg(X^2)$, we have

$$P(X)\,Q(X) = f(X^2)^2 - Xg(X^2)^2.$$

This answers the first part.

One may adopt a similar approach for the second part. Write $P(X) = P_0(X) + XP_1(X) + X^2P_2(X)$ where, for example,

$$P_0(X) = a_0 + a_3X^3 + \dots = f(X^3),$$

$$P_1(X) = a_1 + a_4X^3 + \dots = g(X^3),$$

$$P_2(X) = a_2 + a_5X^3 + \dots = h(X^3).$$

Consider the cube roots of unity $1,\ \omega,\ \omega^2$. If

$$Q_1(X) = P_0(X) + \omega XP_1(X) + \omega^2X^2P_2(X)$$

and

$$Q_2(X) = P_0(X) + \omega^2XP_1(X) + \omega X^2P_2(X),$$

then, using $1 + \omega + \omega^2 = 0$, it is easy to see that

$$R(X) = Q_1(X)\,Q_2(X) = P_0(X)^2 + X^2P_1(X)^2 + X^4P_2(X)^2$$
$$- XP_0(X)\,P_1(X) - X^2P_0(X)\,P_2(X) - X^3P_1(X)\,P_2(X)$$

which is a polynomial with integer coefficients.

Finally,

$$\begin{aligned} P(X)\,R(X) &= \left(P_0(X) + XP_1(X) + X^2P_2(X)\right) \\ &\quad \times \left(P_0(X) + \omega XP_1(X) + \omega^2X^2P_2(X)\right) \\ &\quad \times \left(P_0(X) + \omega^2XP_1(X) + \omega X^2P_2(X)\right) \\ &= P_0(X)^3 + X^3P_1(X)^3 + X^6P_2(X)^3 - 3X^3P_0(X)\,P_1(X)\,P_2(X), \end{aligned}$$

using the identity

$$(l + m + n)(l^2 + m^2 + n^2 - lm - mn - nl) = l^3 + m^3 + n^3 - 3lmn.$$

Thus, since $P_i(X)$ are polynomials are in X^3 for $i = 0,\ 1,\ 2$, we have solved the problem completely.

2. *The polynomial X^k for general k*

The above elementary argument indicates that the case of X^k for general k in place of X^2, X^3 may be cumbersome to approach in this fashion. In this section, we give an elementary proof for the case X^k which is different from the one above for $k = 2, 3$. Following that, we give another less elementary proof for the same and show in the next section that this argument carries over to show, for any non-constant polynomial f in one variable over the integers and for a given polynomial $P(X)$ with integer coefficients, there exist non-zero polynomials $Q(X)$, $R(X)$ with integer coefficients such that $P(X)Q(X)$ is the polynomial $R(f(X))$.

Lemma 1: Let k be a positive integer. Then, for each polynomial $P(X)$ with integer coefficients, there exist non-zero $Q(X)$, $R(X)$ with integer coefficients such that $P(X)Q(X) = R(X^k)$. One has an analogous statement where coefficients are allowed to be rational numbers instead of the integers.

It suffices to prove the version for polynomials over the rational numbers for, if $P(X)$ has integer coefficients and, if we get Q, R with rational coefficients satisfying $P(X)Q(X) = R(X^k)$, then we may multiply out $Q(X)$, $R(X)$ by a suitable integer to get corresponding integral polynomials.

We first give a linear algebraic proof which is illustrated by the following example.

Example: Let $P(x) = 1 + 7x + x^2$ and suppose we wish to find a non-zero $Q(x)$ with integer coefficients such that $P(x)Q(x)$ is of the form $R(x^3)$.

Suppose we try to find rational b_i so that

$$Q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 + b_6x^6$$

works. Then, the coefficients of $x^8, x^7, x^5, x^4, x^2, x$ in $P(x)Q(x)$ are zero. These conditions become the following linear equations for the b_i:

$$\begin{aligned} b_6 &= 0 \\ b_5 &= 0 \\ 7b_4 + b_3 &= 0 \\ b_4 + 7b_3 + b_2 &= 0 \\ b_2 + 7b_1 + b_0 &= 0 \\ b_1 + 7b_0 &= 0. \end{aligned}$$

One non-trivial solution for these 6 equations in 7 variables can be obtained recursively as follows:

$$b_6 = 0, b_5 = 0.$$

Put $b_4 = 1$; then $b_3 = -7$, $b_2 = 48$. Hence $7b_1 + b_0 = -48$, $b_1 + 7b_0 = 0$ which gives $b_1 = -7$, $b_0 = 1$. Therefore,

Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India
e-mail: *sury@isibang.ac.in*

algebraically independent over K if there is no non-zero polynomial p in k variables over K such that $p(t_1, \ldots, t_r) = 0$ in L. A basic fact of the theory is that any two maximal algebraically independent subsets of $K(X_1, \ldots, X_r)$ have the same cardinality, which is called the transcendence degree of L over K (and any such set is called a transcendence base). Moreover, every element of L is algebraic over the subfield generated by K and the transcendence base.

Over a field K, the quotient field $K(X_1, \ldots, X_r)$ of the polynomial ring $K[X_1, \ldots, X_r]$ is the field of all rational functions $\dfrac{f(X_1, \ldots, X_r)}{g(X_1, \ldots, X_r)}$ for non-zero polynomials g. This field $K(X_1, \ldots, X_r)$ has transcendence degree r over K and $\{X_1, \ldots, X_k\}$ is a transcendence base over K.

Proof of theorem: Consider $f_1, \ldots, f_r \in K[X_1, \ldots, X_r]$ as in the statement. The hypothesis means precisely that $\{f_1, \ldots, f_r\}$ is algebraically independent over K (and is, hence, a transcendence base of the field $K(X_1, \ldots, X_r)$ over K). In particular, the field $K(X_1, \ldots, X_r)$ is algebraic over the subfield $K(f_1, \ldots, f_r)$. If its degree is d, then the subset $\{1, P, P^2, \ldots, P^d\}$ of $K(X_1, \ldots, X_r)$ is linearly dependent over $K(f_1, \ldots, f_r)$. In other words, there is a polynomial p in one variable over $K(f_1, \ldots, f_r)$, say

$$p(t) = c_0 + c_1 t + c_2 t^2 + \ldots + c_d t^d$$

with $c_i \in K(f_1, \ldots, f_r)$, such that

$$c_0 + c_1 P + c_2 P^2 + \ldots + c_d P^d = 0 \in K(X_1, \ldots, X_r).$$

By clearing denominators, we may assume that

$$c_i \in K[f_1, \ldots, f_r] \subset K[X_1, \ldots, X_r]$$

for each i.

Writing $Q(X_1, \ldots, X_r) = c_i(f_1, \ldots, f_r) \in K[X_1, \ldots, X_r]$ for $i > 0$ and $Q = Q_1 + Q_2 P + \ldots + Q_d P^{d-1} \in K[X_1, \ldots, X_r]$, we get

$$PQ = Q_1 P + Q_2 P^2 + \ldots + Q_d P^d = -c_0(f_1, \ldots, f_r) \in K[X_1, \ldots, X_r].$$

Taking $R = -c_0$, we have the theorem.

Acknowledgement

The author is indebted to the referee who suggested making the article more readable by adding examples to illustrate the proofs and dividing the material into shorter sections.

Reference

1. P. A. Macmahon, *Combinatory analysis*, Cambridge University Press (1915-1916).

B. SURY

$$Q(x) = 1 - 7x + 48x^2 - 7x^3 + x^4.$$

Note that $P(x)Q(x) = 1 + 322x^3 + x^6$.

First (*linear algebra*) *proof of Lemma* 1

Let $P(X) = \sum_{i=0}^{n} a_i X^i$ be a polynomial of degree n with rational coefficients. Take an arbitrary non-zero polynomial $Q(X) = \sum_{j=0}^{m} b_j X^j$ which is a prospective candidate. The b_j are rational numbers (not all zero) to be determined. Now, expanding out $P(X)Q(X)$, if the coefficients of X^r for $r \leqslant m + n$ with $k \nmid r$ vanish, then it is a polynomial in X^k. Thus, putting the coefficient of X^r in $P(X)Q(X)$ to be zero for each r which is not a multiple of k, there is a homogeneous system of linear equations in the $m + 1$ variables $b_0, b_1, \ldots, b_m$. Since the number of terms X^r with $k \mid r$ is $[(m+n)/k] + 1$, while the total number of terms is $m + n + 1$, the number of equations is $m + n - [(m+n)/k]$. If the number of variables $m + 1$ is larger than $m + n - [(m+n)/k]$, the system is over-determined and has a non-trivial solution for rational b_i. Note that $m + 1 > m + n - [(m+n)/k]$ if, and only if, $[(m+n)/k] + 1 > n$; this happens if $\frac{m+n}{k} > n$.

By choosing m large enough (for example, $m = kn$), it is clear that one has a nontrivial solution for the b_j.

Remark: We note that the above proof gives a polynomial $Q(X)$ of degree at the most kn. Thus, it gives $Q(X)$ of degree at the most $2n$ for the case X^2 and degree at the most $3n$ for the case X^3, whereas the argument in the previous section gave polynomials of degrees n and $2n$ respectively.

Second (*theory of equations*) *proof of Lemma* 1

Consider a polynomial $P(X) = a_0 + a_1 X + \ldots + a_n X^n$ of degree n with rational coefficients. Write $P(X) = a_n \prod_{i=1}^{n} (X - \alpha_i)$ where α_i are the (complex) roots of $P(X)$. Therefore, each coefficient a_i of $P(X)$ is (up to sign) the i th elementary symmetric sum of the roots.

At this point, we recall the classical Girard-Waring identities relating the coefficients a_i of $P(X)$ with the sums $p_r = \sum_{i=1}^{n} \alpha_i^r$ for $r = 1, 2, \ldots, n$ (see [1] for instance):

$$\frac{a_i}{a_n} = \sum \frac{\pm 1}{t_1! \ldots t_i!} \left(\frac{p_1}{1}\right)^{t_1} \ldots \left(\frac{p_i}{i}\right)^{t_i}$$

where the sum is over all t_j with $t_1 + 2t_2 + \ldots + it_i = i$.

This explicit expression is not really relevant but the conclusion that the coefficients are polynomial expressions (with rational coefficients) in the power sums p_r of the roots, is what we need here.

Define $R(X) = a_n \prod_{i=1}^{n} (X - \alpha_i^k)$. Its coefficients are polynomial functions (with rational coefficients) of the numbers $\sum_{i=1}^{n} \alpha_i^{rk}$ for $r \leqslant n$. But $\sum_{i=1}^{n} \alpha_i^{rk}$, for each r, is a polynomial expression (with rational coefficients) in the elementary symmetric functions of the α_i, and hence of the coefficients $\frac{a_i}{a_n}$ of $P(X)$. In other words, the coefficients of $R(X)$ are rational numbers as well.

Consider

$$\frac{R(X^k)}{P(X)} = \prod_{i=1}^{n} \frac{X^k - \alpha_i^k}{X - \alpha_i} = \prod_{i=1}^{n} \left(X^{k-1} + X^{k-2}\alpha_i + \dots + \alpha_i^{k-1}\right).$$

Call this polynomial $Q(X)$. Since $P(X)Q(X) = R(X^k)$ where $P(X)$, $R(X^k)$ are both polynomials with rational coefficients, hence $Q(X)$ must also have rational coefficients by uniqueness of factorisation of polynomials. This finishes the proof.

3. *General polynomial* $f(X)$

The above second proof carries over to a general $f(X)$ in place of X^k. Thus, we can prove:

Lemma 2: Let $f(X)$ be an arbitrary non-constant polynomial with integer coefficients. Then, for each polynomial $P(X)$ with integer coefficients, there exist non-zero $Q(X)$, $R(X)$ with integer coefficients such that $P(X)Q(X) = R(f(X))$. One has an analogous statement with the integers replaced by the rational numbers.

Proof: As before, we may consider the polynomials P, f over the rational numbers. Write

$$P(X) = c \prod_{i=1}^{n} (X - \alpha_i)$$

where the α_i are the roots of $P(X)$. Then, the main observation is that the polynomial

$$R(X) = c \prod_{i=1}^{n} (X - f(\alpha_i))$$

has rational coefficients. This follows as before, because $f(X)$ is a sum of monomials uX^k and, for each X^k, the elementary symmetric functions in the α_i^k are rational numbers as before. In other words, all the coefficients of $R(X)$ (they are elementary symmetric polynomials in the $f(\alpha_1), \dots, f(\alpha_n)$) are rational as well. As $\frac{f(X) - f(\alpha_i)}{X - \alpha_i}$ is a polynomial for each i, $Q(X) = \frac{R(f(X))}{P(X)}$ is a polynomial also. As $R(f(X))$, $P(X)$ have rational coefficients, $Q(X)$ must have rational coefficients by unique factorisation of polynomials. Finally, we observe that $R(f(X))$ is not the zero polynomial since $f(X)$ is not a constant; hence $Q(X)$ is not the zero polynomial.

4. *A multi-variable generalisation*

What we proved earlier is evidently valid over any field K in place of the rational numbers. Now, we go over to an analogous problem for polynomials in more variables. In other words, here is a natural question which can be thought of as a multi-variable version of the earlier problem:

> Let K be any field and let $P \in K[X_1, \dots, X_r]$. Suppose $f_1, \dots, f_r \in K[X_1, \dots, X_r]$ be arbitrary. Do there exist non-zero $Q, R \in K[X_1, \dots, X_r]$ such that
>
> $$P(X_1, \dots, X_r)Q(X_1, \dots, X_r) = R(f_1(X_1, \dots, X_r), \dots f_r(X_1, \dots, X_r))?$$

However, it is easy to see that there must be some restrictions on the f_i in order not to have trivial counter-examples.

Necessary restrictions: If the f_i are constants and if P is not (more generally, if X_1 does not occur in any of the f_i and if P is X_1), then evidently $PQ = R \circ (f_1, \dots, f_r)$ for some Q, R only if $Q = 0 = R \circ (f_1, \dots, f_r)$.

An example: For instance, if $r = 2$, $P = X_1 - X_2$, $f_1 = X_1X_2$, $f_2 = (X_1X_2)^2$, then for any $R \in K[X_1, X_2]$, $R \circ (f_1, f_2)$ is of the form $c_0 + c_1X_1X_2 + \dots + c_k(X_1X_2)^k$. If this is of the form PQ for some $Q \in K[X_1, X_2]$, then one can think of this equality $R \circ (f_1, f_2) = PQ$ in $\overline{K}[X_1, X_2]$ where $\overline{K}$ is an algebraic closure of K. Hence, $R \circ (f_1, f_2)$ vanishes at all points (x, x) as x varies over $\overline{K}$. As these are infinitely many points, this clearly forces all c_i to be zero; that is, $R \circ (f_1, f_2) = 0$. Note that, in fact, $R(X_1, X_2) = X_1^2 - X_2^2$ is non-zero but $R(f_1, f_2) = 0$.

More generally, if $f_1, \dots, f_r$ are algebraically dependent; that is, if there exists $F \neq 0$ in $K[X_1, \dots, X_r]$ such that $F \circ (f_1, \dots, f_r)$ is the zero polynomial, then it can happen that $PQ \neq R \circ (f_1, \dots, f_r)$ for any non-zero Q − indeed, it may even be possible that $R \neq 0$ but $R \circ (f_1, \dots, f_r) = 0 \in K[X_1, \dots, X_r]$. Thus, we may modify the question; we make the modified statement now:

Theorem: Let K be a field and $P \in K[X_1, \dots, X_r]$. Suppose $f_1, \dots, f_r \in K[X_1, \dots, X_r]$ are arbitrary polynomials such that there is no non-zero $F \in K[X_1, \dots, X_r]$ for which $F \circ (f_1, \dots, f_r)$ is the zero polynomial. Then, there exist non-zero Q, $R \in K[X_1, \dots, X_r]$ such that

$$P \cdot Q = R \circ (f_1, \dots, f_r).$$

We recall a few basic facts for the sake of self-containment of the article. To prove the theorem, the basic notion required is that of transcendence bases and transcendence degree.

Let $K \subset L$ be fields; then a subset $S = \{t_1, \dots, t_k\}$ of L is said to be