SOLUTIONS TO PROBLEMS

We discuss some of the problems posed in earlier Newsletters. We begin with Problem 2 in Newsletter #1.

Let $f(x)$ *be a monic polynomial in* $\mathbb{Z}[x]$ *which divides* x^n-1 *and suppose that* a *is a natural number which divides all the coefficients of* $f'(x)$. *Prove that* $f(x) = g(x^a)$ *for some monic integral polynomial* $g(x)$.

Using induction on a, we reduce to the case where $a,=p$ say, is prime.

We first show that $p|n$. For let $x^n-1 = f(x)h(x)$. Differentiate with respect to x and then put $x=\omega$ where ω is a root of $f(x) = 0$ to get $n\omega^{n-1} = f'(\omega)h(\omega)$ and thus n/p is an algebraic integer. So $p|n$.

Let $\Phi_d(x)$ be the cyclotomic polynomial of degree $\phi(d)$. Thus $\Phi_d(x) = (x-\omega_1) \ldots (x-\omega_y)$ where $y = \phi(d)$ and $\omega_1,\ldots,\omega_y$ are the primitive d^{th} roots of 1. We need

(1) if $p^2|d$, $\Phi_d(x) = \Phi_{d/p}(x^p)$.

[To see this, note that if ω is a primitive d^{th} root of 1, then ω^p

is a primitive $(d/p)^{th}$ root of 1. So $\Phi_d(x)$ divides $\Phi_{d/p}(x^p)$. On the other hand, since $p^2|d$. $\phi(d) = p\phi(d/p)$.]

(2) if $p \mid d$, $\Phi_{pd}(x) = \Phi_d(x^p)/\Phi_d(x)$

[To see this, note that if ω is a primitive d^{th} root of 1, so is ω^p since $p \mid d$. So $\Phi_d(x)$ divides $\Phi_d(x^p)$. Also, as above, $\Phi_{pd}(x)$ divides $\Phi_d(x^p)$. But $\phi(pd) = (p-1)\phi(d) = p\phi(d)-\phi(d) = \deg \Phi_d(x^p) - \deg \Phi_d(x)$, so (2) follows.]

Now $f(x)$ divides x^n-1, so we may write $f(x)$ as a product of $\Phi_d(x)$'s for various d's dividing n. We write

$$f(x) = \left[\prod_{p|d} \Phi_d(x)\right]\left[\prod_{p|e} \Phi_{pe}(x)\right]\left[\prod_{p^2|g} \Phi_g(x)\right]$$

(where some of the products may be empty).

Using (1),(2), we may write

$$f(x) = \left[\frac{\prod_{p\nmid d_o} \Phi_{d_o}(x)}{\prod_{p\nmid e_o} \Phi_{e_o}(x)}\right] \cdot \left[\prod_{p\nmid e} \Phi_e(x^p) \prod_{p|g} \Phi_{g/p}(x^p)\right]$$

$$= \left[\frac{u(x)}{v(x)}\right] \cdot k(x^p), \quad \text{say,}$$

where $(u(x),v(x)) = 1$.

Differentiating we thus find that p divides all the coefficients of $v(x)u'(x)-u(x)v'(x)$. Now since p does not divide any of the indices m for which $\Phi_m(x)$ occurs in $u(x)v(x)$ and $(u(x),v(x))=1$, $u(x)v(x)$ divides x^r-1 for some r with $p|r$. But then if $u(x)v(x)\neq 1$, writing $x^r-1 = u(x)v(x)w(x)$, differentiating and putting $x=\zeta$ where ζ is a root of $u(x)v(x)=0$ we get a contradiction as in the first paragraph. Hence $u(x)v(x)=1$ and $u(x)=1=v(x)$. This proves the result.

This result is due to Leonard Scott. His proof uses modular character theory (see Proc. of the Park City, Utah, Conference on Finite Groups).

We now discuss Problem 10 on Newsletter #1.

Let G *be a finite abelian group of order* n *and let* $g_1,\ldots,g_{2n-1}$ *be elements of* G. *Prove that there exists a subsequence* $g_{r_1},\ldots,g_{r_n}$ *of exactly* n *g's with* $g_{r_1}\ldots g_{r_n}=1$.

Let A be a subset of a group X. We write $|A|$ to denote the number of elements in A. Given non-empty subsets A,B we write $AB=\{ab|a\in A,b\in B\}$.

We use the following result of Cauchy:

Let X be the cyclic group of prime order p and let A,B be non-empty subsets of X. Then either $AB=X$ or $|AB|\geq |A|+|B|-1$. (For a proof, see a paper of Davenport (Journal of the London Math. Soc. (1937).)

Suppose that G has prime order p and let $A = \{g_1,\ldots,g_{2p-1}\}$. Let $A^2 = AA$, etc. Note that if $A^k \neq G$ for $1 \leq k \leq p$, then $|A^p| \geq p|A|-p+1 > |G|$ unless $|A| = 1$. If $A = 1$, the result is obvious. Assume $A \neq 1$, then $A^k = G$ for some k with $1 \leq k \leq p$ and thus $A^{k+1} = AG = G$, etc. So $A^p = G$. So the result holds in this case.

In the general case we use induction on $|G|$. Let p be a prime divisor of $|G|$ and let L be a subgroup of order p. Applying the induction hypothesis we find $g_{r_1},\ldots,g_{r_{n/p}}$ among the first $2(\frac{n}{p}) - 1$ of the g's with $w_1 = g_{r_1}+\ldots+g_{r_{n/p}} \in L$. We apply the induction hypothesis to the sequence obtained by deleting $g_{r_1},\ldots,g_{r_{n/p}}$ in the original sequence to get $2 = g_{s_1}+\ldots+g_{s_{n/p}} \in L$. Proceed thus. Note that since $2n-1 = \frac{n}{p}(2p-2)+2(\frac{n}{p})-1$ we can construct $w_1,\ldots,w_{2p-1}$ in this way. Applying the theorem to L and the sequence $w_1,\ldots,w_{2p-1}$ now gives a subsequence $z_1+\ldots+z_p = 1$. But each z_i is a sum of $\frac{n}{p}$ elements of the original sequence and z_i, z_j $(i \neq j)$ involve g's with entirely different indices. The result follows. [This result is due to Erdos, Ginzburg and Ziv.]

Problem 6 of Newsletter #1 asked the following:

Let A,B *be* $n \times n$ *(complex) matrices such that* $AB-BA$ *has rank one. Prove that* A,B *have a common eigenvector (i.e. there exists a vector* $v \neq 0$ *such that* $Av = \lambda v$, $Bv = \mu v$ *for some* λ,μ*).*

The solution of this problem was discussed in Newsletter #2, where it was remarked that no short elementary proof was known. In a paper to appear in Linear & Multilinear Alg., M.-D. Choi, C. Laurie and H. Radjavi have provided such a proof. The key observation is

Theorem If A,B are any linear operators on a vector space V and if $AB-BA$ has rank one, then either the null-space or range of A is invariant under B.

Proof Assume that the null-space N of A is not invariant under B. (Note that this implies in particular that N is nontrivial, i.e. $0 \neq N \neq V$.) Then there exists a non-zero vector x in V with $Ax = 0$ and $ABx \neq 0$. Then $(AB-BA)x = ABx$ spans the (one-dimensional) range of $AB-BA$ and, for every $y \in V$, there exists a scalar λ_y such that

$$(AB-BA)y = \lambda_y ABx.$$

It follows that $BAy = AB(y-\lambda_y x)$, yielding

$$BAV \subseteq ABV \subseteq AV$$

as desired.

Let λ be an eigenvalue of A. Then

$$AB-BA = (A-\lambda I)B-B(A-\lambda I)$$

and the kernel and null-space of $A-\lambda I$ are proper subspaces of V. So V has a proper (A,B) - invariant subspace. The result of Q.6 now follows by induction.

I am grateful to Choi, Laurie and Radjavi for providing me with a preprint of their paper entitled "Commutators and invariant subspaces". Their paper contains extensions of the result to infinite dimensional spaces.

We now discuss two of the problems posed in Newsletter #2.

(2.2) *Prove that if* c *is a real number such that* n^c *is a natural number for every natural number* n, *then* c *is a non-negative integer.*

Let k be a natural number $>c$. Let $f(x) = x^c$. Note that $\sum_{r=0}^{k} (-1)^r \binom{k}{r} f(x+rh) = (-h)^n f^{(k)}(\xi)$ for some ξ between x and $x+kh$ [cf. Eggleston Elementary Real Analysis CUP (1962), page 119]. Let $h=1$. Then

$$\sum_{r=0}^{k} (-1)^r \binom{k}{r} (x+r)^c = (-1)^n c(c-1) \ldots (c-k+1)\xi^{c-k}$$

where

$$x<\xi<x+k.$$

Let $x \to \infty$ through the set of natural numbers. By hypothesis, the left-hand side of (*) is an integer while the right-hand side tends to zero (since $k>c$). Hence the right-hand side is zero for some large x and thus c is one of the numbers $0,1,2,\ldots,k-1$.

[This problem was posed in the Putnam Examination in 1971.]

(2.8) *Let* $f(x), g(x)$ *be monic integral polynomials and let* α, β *be roots of* $f(x), g(x)$, *respectively (in the complex field). Suppose* α, β *can both be expressed as integral linear combinations of square roots of integers. Prove that there exist integral polynomials* $h(x), k(x)$ *such that h.c.f.* $(f(h(x)), g(k(x)))$ *has degree greater than one. Generalize.*

Let $f_0(x), g_0(x)$ be irreducible factors of $f(x), g(x)$, respectively such that α is a root of $f_0(x)$, β a root of $g_0(x)$. Note that the conclusion for $f(x), g(x)$ will follow from that for $f_0(x), g_0(x)$. Thus we

may assume that $f(x), g(x)$ are irreducible. Note that the forms of α, β imply that $Q(\alpha, \beta)$ is a normal extension of Q with abelian Galois group. By a theorem of Kronecker (Lang Algebraic Number Theory, p.210), $Q(\alpha, \beta) \subseteq Q(\omega)$ where $\omega^n = 1$ for some n. The set of algebraic integers in $Q(\omega)$ is just $Z[\omega]$ (Lang, ibid., p.75), so there exist integral polynomials $h(x), k(x)$ such that $\alpha = h(\omega)$, $\beta = k(\omega)$. But then ω is a root of $f(h(x))$ and also a root of $g(k(x))$. The result follows.

This problem was posed by Robert Gilmer (Tallahassee). He asks whether the result holds without any restriction on the form of α, β. This more general question appears to be open at present.