TOPICS IN MATHEMATICS
PROBLEM SET 3 SOLUTIONS

PAUL L. BAILEY

Problem 1. Let $m, n \in \mathbb{Z}$ be nonzero and suppose that there exist integers $x, y \in \mathbb{Z}$ such that $mx + ny = 1$. Show that $\gcd(m, n) = 1$.

Solution. We know that if $\gcd(m, n) = d$, then there exist $x, y \in \mathbb{Z}$ such that $mx + ny = d$. However, the converse is not true in general. For example, let $m = 2$ and $n = 3$. Then it is the case that

$$5m + 2n = 16,$$

but it is not the case that $\gcd(m, n)$ is 16.

However, if $mx + ny = 1$, then it follows that $\gcd(m, n) = 1$, as we now demonstrate.

Suppose that $mx + ny = 1$ for some $x, y \in \mathbb{Z}$. Let $d = \gcd(m, n)$. Then d divides m and d divides n, so $m = da$ and $n = db$ for some $a, b \in \mathbb{Z}$. Then $dax + dby = 1$, do d divides 1. The only positive integer which divides 1 is 1; thus $d = 1$. □

Problem 2. Let $f(x) = x^2 + 46x + 54$. Show that f is irreducible over $\mathbb{Q}$, but is reducible over $\mathbb{Z}_{17}$.

Solution. Recall *Eisenstein's criterion*, which say that f is a polynomial with integer coefficients, and p is a prime integer satisfying:

- **(a)** the leading coefficient of f is not divisible by p,
- **(b)** every other coefficient of f is divisible by p,
- **(c)** the constant coefficient of f is not divisible by p^2,

then f is irreducible other $\mathbb{Z}$, and consequently is irreducible other $\mathbb{Q}$ by Gauss' lemma.

Note $46 = 2 \cdot 23$ and $54 = 2 \cdot 3^3$, so f satisfies the hypothesis of Eisenstein's criterion with $p = 2$. Thus f is irreducible over $\mathbb{Q}$.

Let $\overline{f}$ be the residue of f modulo 17. We have $46 \equiv 12 \equiv -5 \pmod{17}$ and $54 \equiv 3 \equiv -14 \pmod{17}$. Thus

$$\overline{f}(x) = x^2 - 5x - 14 = (x - 7)(x + 2).$$

Thus $\overline{f}$ is reducible. □

Date: December 6, 2006.

Problem 3. Let $\beta = \sqrt[3]{\sqrt{2}+\sqrt{3}}$.

(a) Find the minimum polynomial of β over $\mathbb{Q}$.

(b) Find the minimum polynomial of β over $\mathbb{Q}[\sqrt{6}]$.

Solution. Compute $\beta^3 = \sqrt{2}+\sqrt{3}$, so $\beta^6 = 5+2\sqrt{6}$, whence $(\beta^6-5)^2 = 24$. Writing this in standard form, we obtain

$$\beta^1 2 - 10\beta^6 + 1 = 0.$$

Let $f(x) = x^1 2 - 10x^6 + 1$; then $f(\beta) = 0$. Thus f is a monic polynomial which annihilates β; we wish to show that f is irreducible over $\mathbb{Q}$. Since we know that the minimum polynomial of β is divisible by f, it suffices to show that the degree of the minimum polynomial of β is 12. We also know that the degree of the minimum polynomial is equal to the degree of the corresponding primitive extension.

We show that $[\mathbb{Q}[\beta] : \mathbb{Q}] = 12$ by using the product of degrees formula.

The minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, so $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. It is impossible to solve the equation $\sqrt{3} = a + b\sqrt{2}$ for rational numbers a and b, so $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

The minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $x^2 - 3$; but since $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ and $x^2 - 3$ is quadratic, it cannot possibly factor over $\mathbb{Q}[\sqrt{2}]$. Thus $x^2 - 3$ is irreducible over $\mathbb{Q}[\sqrt{3}]$, which shows that

$$[\mathbb{Q}[\sqrt{2},\sqrt{3}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{2},\sqrt{3}] : \mathbb{Q}[\sqrt{2}]][\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Let $\alpha = \sqrt{2}+\sqrt{3}$; we show that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2},\sqrt{3}]$. It is clear that $\alpha \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$, so we show that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}[\alpha]$.

Set $h(x) = x^4 - 10x^2 + 1$. Then h is a polynomial which annihilates α, so α is algebraic over $\mathbb{Q}$, so $\mathbb{Q}[\alpha]$ is a field. The inverse of α is also in $\mathbb{Q}[\alpha]$, and may be computed as

$$\alpha^{-1} = \frac{1}{\sqrt{3}+\sqrt{2}} = \frac{\sqrt{3}-\sqrt{2}}{3-2} = \sqrt{3}-\sqrt{2}.$$

Thus $\dfrac{\alpha+\alpha^{-1}}{2} = \sqrt{3} \in \mathbb{Q}[\alpha]$, and consequently $\alpha - \sqrt{3} = \sqrt{2} \in \mathbb{Q}[\alpha]$. Conclude that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2},\sqrt{3}]$. Incidently, this also shows that h is irreducible over $\mathbb{Q}$, and that $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$.

Finally, it is clear that $\beta \notin \mathbb{Q}[\alpha]$. However, $x^3 - \alpha$ is a polynomial over $\mathbb{Q}[\alpha]$ which annihilates β. This cubic polynomial is irreducible unless it has a root in $\mathbb{Q}[\alpha]$. But the roots are β, $\beta\omega$, and $\beta\omega^2$, where $\omega = e^{2\pi i/3}$. The latter two are nonreal, and so are certainly not in the real field $\mathbb{Q}[\alpha]$. Thus $x^3 - \alpha$ is the minimum polynomial of β over $\mathbb{Q}[\alpha]$. Thus

$$[\mathbb{Q}[\beta] : \mathbb{Q}] = [\mathbb{Q}[\beta] : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}] = 3 \cdot 4 = 12.$$

This details why $f(x) = x^{12} - 10x^6 + 1$ must be irreducible over $\mathbb{Q}$.

Looking back at our initial computation, we see that $\beta^6 - 5 - 2\sqrt{6} = 0$. Thus let $g \in \mathbb{Q}[\sqrt{6}]$ be given as $g(x) = x^6 - (5 + 2\sqrt{6})$. Since $[\mathbb{Q}[\sqrt{6}] : \mathbb{Q}] = 2$, we must have $[\mathbb{Q}[\beta] : \mathbb{Q}[\sqrt{6}] = 12/2 = 6$. Thus g is irreducible. $\square$

Problem 4. Let $\beta = e^{2\pi/16}$.

(a) Find the minimum polynomial of β over $\mathbb{Q}$.
(b) Find the minimum polynomial of β over $\mathbb{Q}[i]$.
(c) Find the minimum polynomial of β over $\mathbb{Q}[\sqrt{2}]$.

Solution. Since $\beta^8 = e^{\pi i} = -1$, we see that β is a root of $f(x) = x^8 + 1$. We wish to show that f is irreducible, again by computing degrees.

Now $\beta = \operatorname{cis}(2\pi i/16) = \cos(2\pi i/16) + i\sin(2\pi i/16)$; use the half angle formula to compute

$$\beta = \frac{\sqrt{2-\sqrt{2}}}{2} + i\frac{\sqrt{2+\sqrt{2}}}{2}.$$

Note that $\beta^2 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, and $\beta^4 = i$. Then $i, \sqrt{2}, \sqrt{2+\sqrt{2}} \in \mathbb{Q}[\beta]$.

Drawing on previous experience, we can see that $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, but that $\sqrt{2+\sqrt{2}} \notin \mathbb{Q}[\sqrt{2}]$. Thus $[\mathbb{Q}[\sqrt{2+\sqrt{2}}] : \mathbb{Q}] = 4$. Since $\sqrt{2+\sqrt{2}} \in \mathbb{R}$, the field it generates over $\mathbb{Q}$ is also contained in $\mathbb{R}$, and in particular, does not contain i. Thus $[\mathbb{Q}[i, \sqrt{2+\sqrt{2}}] : \mathbb{Q}] = 8$, which proves that f is irreducible.

The minimum polynomial of β over $\mathbb{Q}[i]$ must be of degree 4, and $\beta^4 = i$. Thus, $x^4 - i$ is the minimum polynomial of β over $\mathbb{Q}[i]$.

The minimum polynomial of β over $\mathbb{Q}[\sqrt{2}]$ also is of degree 4; note that $\overline{\beta} = \beta^{-1}$ is the complex conjugate of β, so

$$\beta + \beta^{-1} = 2\Re(\beta) = \sqrt{2-\sqrt{2}}.$$

Squaring gives $\beta^2 + 2 + \beta^{-2} = 2 - \sqrt{2}$, so $\beta^4 + \sqrt{2}\beta^2 + 1 = 0$. Thus $x^4 + \sqrt{2}x^2 + 1$ is the minimum polynomial of β over $\sqrt{2}$. □

Problem 5. Let $f(x) = x^{12} - 1$, and let $E \subset \mathbb{C}$ be the splitting field of f over $\mathbb{Q}$. Write E as a multiple extension, and find $[E : \mathbb{Q}]$.

Solution. Let

$$\beta = e^{2\pi i/12} = \frac{\sqrt{3}}{2} + i\frac{1}{2}.$$

Since β is a primitive twelfth root of unity, all the other roots of f are powers of β, so $E = \mathbb{Q}[\beta] = \mathbb{Q}[\sqrt{3}, i]$. Thus $[E : \mathbb{Q}] = 4$.

Let's find the minimum polynomial of β over $\mathbb{Q}$, by way of factoring f into irreducible polynomials:

$$\begin{aligned} x^{12} - 1 &= (x^6 - 1)(x^6 + 1) \\ &= (x^3 - 1)(x^3 + 1)(x^2 + 1)(x^4 - x^2 + 1) \quad \text{(sum of cubes formula)} \\ &= (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)(x^2 + 1)(x^4 - x^2 + 1). \end{aligned}$$

The last factor is the only one whose degree is at least four; thus it must be the minimum polynomial of β over $\mathbb{Q}$, and is irreducible. We identify the powers of β which are roots of each of these polynomials:

- 1, the primitive first root of unity, is a root of $x - 1$;
- -1, the primitive second root of unity, is a root of $x + 1$;
- β^4, β^8, the primitive cube roots of unity, are roots of $x^2 + x + 1$;
- β^2, β^{10}, the primitive sixth roots of unity, are roots of $x^2 - x + 1$;
- $\pm\beta^3 = \pm i$, the primitive fourth roots of unity, are roots of $x^2 + 1$;
- $\beta, \beta^5, \beta^7, \beta^{11}$, the primitive twelfth roots of unity, are roots of $x^4 - x^2 + 1$.

□

Problem 6. Let K/E and E/F be algebraic extensions. Show that K/F is an algebraic extension.

Solution. Recall that an element of K is *algebraic* over F if it is a root of a polynomial with coefficients in F, and that K/F is an algebraic extension if every element of K is algebraic over F.

Let $\beta \in K$; we wish to show that β is algebraic over F. Since K/E is an algebraic extension, β is algebraic over E, so there exists $g \in E[x]$ such that $g(\beta) = 0$. Since $g \in E[x]$, there exist $\alpha_0, \ldots, \alpha_n \in E$ such that

$$g(x) = \sum_{i=0}^{n} \alpha_i x^i.$$

Since E/F is an algebraic extension, α_i is algebraic over F for $i = 0, \ldots, n$.

Let $L = F[\alpha_0, \ldots, \alpha_n]$. Then $f \in L[x]$ and $f(\beta) = 0$, so β is algebraic over L, and $L[\beta]/L$ is a finite extension whose degree is less than or equal to n (it is equal to n if f is irreducible over L).

Also, L is a multiple extension of F, and therefore is finite. Now

$$[L[\beta] : F] = [L[\beta] : L][L : F] < \infty,$$

so $L[\beta]/F$ is a finite extension, and therefore is an algebraic extension. Thus β is algebraic over F. □

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu