Problem of the Month

Solution to Problem 6: March 2024

(a) Notice that $f(2) = 2^4 - 2(2)^3 - 2(2)^2 + 8 = 16 - 16 - 8 + 8 = 0$, so 2 is a root of $f(x)$. This means $(x-2)$ is a factor of $f(x)$. Factoring gives $f(x) = (x-2)(x^3 - 2x - 4)$. Now evaluating $2^3 - 2(2) - 4 = 8 - 4 - 4 = 0$, we get that 2 is a root of $x^3 - 2x - 4$, so $(x-2)$ is a factor of $x^3 - 2x - 4$. Factoring gives $x^3 - 2x - 4 = (x-2)(x^2 + 2x + 2)$.

Applying the quadratic formula to $x^2 + 2x + 2$ gives

$$\frac{-2 \pm \sqrt{2^2 - 4(2)}}{2} = \frac{-2 \pm \sqrt{-4}}{2} = \frac{-2 \pm 2i}{2} = -1 \pm i$$

So the roots of $f(x)$ are 2, $-1+i$, and $-1-i$ with 2 appearing as a repeated root.

(b) This polynomial has no real roots, but notice that $g(x) = x^4 + 2x^2 + 1 = (x^2+1)^2$. The roots of $x^2 + 1$ are $\pm i$, so the only roots of $g(x)$ are i and $-i$. In fact, $g(x)$ can be factored as $g(x) = (x-i)^2(x+i)^2$ which shows that each of these two roots are repeated roots.

(c) We can use a difference of square to get that $h(x) = (x^2+2)(x^2-2)$. The roots of $x^2 - 2$ are $\sqrt{2}$ and $-\sqrt{2}$. The roots of $x^2 + 2$ are $i\sqrt{2}$ and $-i\sqrt{2}$. Thus, $h(x)$ has four distinct roots (no repeated roots), two of which are real and two of which are not real.

Notation: In several of the remaining solutions, we will use the word *monic* to describe a polynomial with a leading coefficient of 1. One of the main observations about monic polynomials is that if $p(x)$ is a polynomial with leading coefficient $a \neq 0$, then $\frac{1}{a}p(x)$ is a monic polynomial of the same degree with exactly the same roots as $p(x)$. We will leave the following fact as an exercise: If $p(x)$ is a reducible monic polynomial, then $p(x)$ factors as the product of two monic polynomials of degree at least 1.

(d) (i) **The polynomial is irreducible**. Suppose $x^2 - 2$ is reducible. Since the polynomial is monic, there must be monic rational polynomials $p(x)$ and $q(x)$ of degree at least 1 such that $p(x)q(x) = x^2 - 2$. Since $p(x)$ and $q(x)$ both have degree at least 1 and their product has degree 2, they must both have degree exactly 1.

Therefore, there are rational numbers a and b such that $p(x) = x + a$ and $q(x) = x + b$, so $x^2 - 2 = (x+a)(x+b)$. Expanding, we get $x^2 - 2 = x^2 + (a+b)x + ab$. Comparing coefficients, $a + b = 0$ or $a = -b$, and $ab = -2$. Substituting $a = -b$ into $ab = -2$ gives $-b^2 = -2$ or $b^2 = 2$. It is well known that no rational number b has the property that $b^2 = 2$, and so there is a problem. We conclude that $x^2 - 2$ cannot be factored into the product of two rational polynomials both with positive degree.

Observation: It is important to observe that we have specifically shown that $x^2 - 2$ does not factor over $\mathbb{Q}$. If we allow for any real coefficients, we easily get that $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ which is a perfectly good factorization into a product of polynomials with real coefficients. Extending the language defined in the problem, we would say that while $x^2 - 2$ is irreducible over $\mathbb{Q}$, it is reducible over $\mathbb{R}$.

(ii) **The polynomial is reducible**. Checking for rational roots and then factoring, one finds that $x^3 - 6x^2 + 11x - 6 = (x-1)(x-2)(x-3)$.

(iii) **The polynomial is irreducible**. If a cubic polynomial is equal to the product of polynomials $p(x)$ and $q(x)$ each with degree at least 1, then one of them must be linear and the other must be quadratic. This is because $1 + 2$ is the only way to express 3 (the degree) as the sum of positive integers. Since x^3+x+1 is monic, there must be rational numbers a, b, and c so that $x^3 + x + 1 = (x + a)(x^2 + bx + c)$. Of course, this shows that $-a$ is a rational root, so we get the following useful fact that is special to cubics (and quadratics): A cubic polynomial is reducible over $\mathbb{Q}$ if and only if it has a rational root.

By the rational root theorem, 1 and -1 are the only candidates for a rational root of $x^3 + x + 1$. Neither is a root, so the polynomial has no rational roots. Therefore, by the argument above, the polynomial is irreducible.

(iv) **The polynomial is irreducible**. Every linear polynomial is irreducible. This is because the product of two polynomials of positive degree must have degree at least 2, so a polynomial of degree less than 2 cannot possibly be expressed as the product of two polynomials of positive degree.

(v) **The polynomial is reducible**. Observe that $x^4+3x^2+2 = (x^2+1)(x^2+2)$, and so $x^4 + 3x^2 + 2$ can be expressed as the product of two rational polynomials of positive degree.

The roots of the polynomial are i, $-i$, $i\sqrt{2}$ and $-i\sqrt{2}$, none of which are real. In part (iii) above, it was noted that a rational cubic is irreducible over $\mathbb{Q}$ if and only if it has a rational root. This example shows that this is special property of polynomials of low degree since $x^4 + 3x^2 + 2$ is reducible, but it does not have any rational roots.

(vi) **The polynomial is irreducible**. If $x^4+1 = 0$, then $(x^2)^2 = -1$, which is impossible for a real number x. Therefore, x^4+1 has no rational roots (since it has no real roots).

If $x^4 + 1$ factors as the product of two rational polynomials of positive degree, then it must be the product of a linear with a cubic, or the product of two quadratics. The polynomial has no rational root, so it has no linear factor, which means the only remaining possibility is that $x^4 + 1$ is the product of two rational quadratics. As mentioned earlier, if a monic polynomial factors, then it factors as the product monic polynomials.

We will assume that a, b, c, and d are real numbers such that $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ and deduce that these numbers cannot all be rational.

Expanding, we have

$$x^4 + 1 = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$$

and by comparing coefficients, we get

$$a + c = 0 \qquad (1)$$

$$ac + b + d = 0 \qquad (2)$$

$$ad + bc = 0 \qquad (3)$$

$$bd = 1 \qquad (4)$$

From Equation (1), we get $a = -c$ and so we can substitute into Equations (2) and (3) above to get

$$-c^2 + b + d = 0 \tag{2'}$$
$$-cd + bc = 0 \tag{3'}$$

If $c = 0$, then Equation (2') implies $b = -d$, and substituting into Equation (4) gives $-d^2 = 1$ or $d^2 = -1$. This means $d = i$ or $d = -i$, neither of which is rational.

If $c \neq 0$, then we can divide through by c in Equation (3') to get $-d + b = 0$ or $b = d$. Equation (4) now implies that $b^2 = d^2 = 1$, so either $b = d = 1$ or $b = d = -1$.

If $b = d = 1$, then Equation (2') gives $-c^2 + 2 = 0$ or $c^2 = 2$, so $c = \pm\sqrt{2}$. Either way, c is irrational.

If $b = d = -1$, then Equation (2') gives $c^2 = -2$ and so $c = \pm i\sqrt{2}$, both of which are irrational.

We have exhausted all possibilities and deduced that at least one of a, b, c, and d must be irrational in all cases, so we have shown that $x^4 + 1$ cannot possibly factor as the product of two rational quadratic polynomials.

If you look a bit more closely at the case work above, it actually shows that $x^4 + 1$ has the following three different factorizations:

$$x^4+1 = (x^2+i)(x^2-i) = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1) = (x^2-i\sqrt{2}x-1)(x^2+i\sqrt{2}x-1)$$

but none of them are factorizations into rational polynomials.

(e) The real number $\sqrt{2}$ is algebraic because it is a root of the rational polynomial $x^2 - 2$.

To find a rational polynomial to which $1+\sqrt[3]{2}$ is a root, we write $r = 1+\sqrt[3]{2}$ and rearrange to get $r - 1 = \sqrt[3]{2}$. Cubing both sides, we get $r^3 - 3r^2 + 3r - 1 = 2$. We can rearrange this to see that $r^3 - 3r^2 + 3r - 3 = 0$, which shows that $r = 1 + \sqrt[3]{2}$ is a root of the polynomial $x^3 - 3x^2 + 3x - 3$, which is a rational cubic.

Let $\alpha = 1 + 2i$ and $\beta = 1 - 2i$. Notice that $\alpha + \beta = 2$ and $\alpha\beta = (1 + 2i)(1 - 2i) = 1^2 - (2i)^2 = 5$. The polynomial $(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta = x^2 - 2x + 5$, a rational quadratic, has $\alpha = 1 + 2i$ as a root by construction.

For $\sqrt{2}+\sqrt{3}$, we will use a similar trick to that which was used for $1+\sqrt[3]{2}$. Set $r = \sqrt{2}+\sqrt{3}$ and rearrange to get $r - \sqrt{2} = \sqrt{3}$. Squaring both sides gives $r^2 - 2\sqrt{2}r + 2 = 3$ which can be rearranged to get $r^2 - 1 = 2\sqrt{2}r$. Squaring both sides again gives $r^4 - 2r^2 + 1 = 8r^2$, which can be rearranged to $r^4 - 10r^2 + 1 = 0$. Therefore, $\sqrt{2} + \sqrt{3}$ is a root of the rational polynomial $x^4 - 10x^2 + 1$.

The degrees of $\sqrt{2}$, $1 + \sqrt[3]{2}$, $1 + 2i$, and $\sqrt{2} + \sqrt{3}$ are 2, 3, 2, and 4, respectively. We will justify this at the end of the solution to part (j).

(f) Suppose α is an algebraic number of degree d. It follows from the remark before the solution to part (d) that there is a rational monic polynomial $p(x)$ of degree d such that $p(\alpha) = 0$.

Suppose $p(x)$ is reducible over $\mathbb{Q}$. Then there are rational polynomials $f(x)$ and $g(x)$ such that $p(x) = f(x)g(x)$ and both $f(x)$ and $g(x)$ have degree at least 1. Since the sum of the degrees of $f(x)$ and $g(x)$ is d, it follows that each of them has degree less than d.

Since $p(\alpha)=0$, we get $0 = f(\alpha)g(\alpha)$, and so either $f(\alpha) = 0$ or $g(\alpha) = 0$. This is impossible since d is the smallest positive degree of a rational polynomial having α as a root.

This shows $p(x)$ is irreducible, so we have shown that there exists a monic irreducible rational polynomial of degree d with $p(\alpha) = 0$.

Now we want to show that that is only one such polynomial. To do this, suppose $p(x)$ and $q(x)$ are monic irreducible polynomials of degree d such that $p(\alpha) = q(\alpha) = 0$. Let $h(x) = p(x) - q(x)$. Since $p(x)$ and $q(x)$ have the same leading term, x^d, the degree of $h(x)$ must be less than d. As well, $h(\alpha) = p(\alpha) - q(\alpha) = 0$, so α is a root of a polynomial with degree less than d. By the definition of d, $h(x)$ cannot have positive degree, so it must be constant. The only constant polynomial with roots is the constant zero polynomial, so $h(x) = p(x) - q(x) = 0$ for all x, from which it follows that $p(x) = q(x)$.

We have assumed that two monic irreducible polynomials of degree d have α as a root and deduced that they are the same polynomial. We conclude that there is a *unique* monic irreducible polynomial $m(x)$ of degree d such that $m(\alpha) = 0$.

(g) By looking for rational roots and removing corresponding factors, we arrive at

$$f(x) = (x+1)(x-2)^2(x^4 + 2x^2 + 1)$$

In part (b), it was observed that $x^4 + 2x^2 + 1 = (x^2 + 1)^2$, so $f(x)$ factors completely as

$$f(x) = (x+1)(x-2)^2(x-i)^2(x+i)^2$$

and so the values of r_1, r_2, r_3, r_4, r_5, r_6, r_7 are -1, 2, 2, i, i, $-i$, $-i$.

(h) (i) Expanding $(x+y)^n$ for each n from 2 through 7, we have

$$\begin{aligned}
(x+y)^7 &= x^7 + 7x^6y + 21x^5y^2 + 35x^4y^3 + 35x^3y^4 + 21x^2y^5 + 7xy^6 + y^7 \\
(x+y)^6 &= x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6 \\
(x+y)^5 &= x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5 \\
(x+y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \\
(x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 \\
(x+y)^2 &= x^2 + 2xy + y^2
\end{aligned}$$

Substituting $x + y$ for x in $f(x)$, we get

$$f(x+y) = (x+y)^7 - 3(x+y)^6 + 2(x+y)^5 - 2(x+y)^4 + (x+y)^3 + 5(x+y)^2 + 4$$

Without actually substituting the expressions for $(x+y)^2$ through $(x+y)^7$ from above, we can imagine what will happen if we do. The polynomial $f_0(x)$ is equal to the sum of the terms we would get that have no factor of y. The only term in $(x+y)^n$ that does not have a factor of y is x^n. Therefore, we can conclude that

$$f_0(x) = x^7 - 3x^6 + 2x^5 - 2x^4 + x^3 + 5x^2 + 4$$

which is $f(x)$, the roots of which were found in the previous part.

The polynomial $f_1(x)$ has the property that $yf_1(x)$ is the sum of all terms that have a factor of y and the exponent of y is exactly 1. In $(x+y)^n$, this term is always of the form $nx^{n-1}y$.

Therefore, we can collect all terms that have exactly one factor of y in $f(x+y)$ to get

$$\begin{aligned} yf_1(x) &= 7x^6y - 3(6x^5y) + 2(5x^4y) - 2(4x^3y) + (3x^2y) + 5(2xy) \\ &= y(7x^6 - 18x^5 + 10x^4 - 8x^3 + 3x^2 + 10x) \end{aligned}$$

So we conclude that $f_1(x) = 7x^6 - 18x^5 + 10x^4 - 8x^3 + 3x^2 + 10x$.

After checking for rational roots, one finds that $f_1(x) = x(x-2)(7x^4 - 4x^3 + 2x^2 - 4x - 5)$ and that $h(x) = 7x^4 - 4x^3 + 2x^2 - 4x - 5$ has no rational roots. However, a bit of experimentation or observation leads to

$$\begin{aligned} h(i) &= 7(i)^4 - 4i^3 + 2i^2 - 4i - 5 \\ &= 7(-1)^2 - 4(-1)i + 2(-1) - 4i - 5 \\ &= 7 + 4i - 2 - 4i - 5 \\ &= 0 \end{aligned}$$

and one can check that $h(-i) = 0$ as well. Thus, we should be able to factor $(x-i)$ and $(x+i)$ out of $h(x)$, but $(x-i)(x+i) = x^2+1$, so we can factor x^2+1 out of $h(x)$ and avoid arithmetic with complex numbers. After doing this, we find $h(x) = (x^2+1)(7x^2-4x-5)$. Using the quadratic formula on $7x^2-4x-5$ gives $x = \dfrac{2 \pm \sqrt{39}}{7}$. We have now found all roots of $f_1(x)$ and they are 0, 2, i, $-i$, $\dfrac{2+\sqrt{39}}{7}$, and $\dfrac{2-\sqrt{39}}{7}$. Observe that 2, i, and $-i$ were all repeated roots of $f(x)$ (from part (g)) and they all appear as roots of $f_1(x)$.

(ii) In general, $f(x+y)$ can be expressed as

$$f(x+y) = f(x) + f_1(x)y + X$$

where X is some expression that is the sum of products of scalars, powers of x, and powers of y. However, since $f(x)$ and $f_1(x)y$ are the collections of terms that have no factor of y and exactly one factor of y, we can conclude that X has a factor of y^2. Therefore, we can refine this observation to get that $f(x+y) = f(x) + f_1(x)y + y^2\overline{f}(x,y)$ where $\overline{f}(x,y)$ is the sum of terms that are products of scalars, powers of x, and powers of y. Note that if $f(x)$ is constant, then $f_1(x)$ and $\overline{f}(x,y)$ will be 0, and if $f(x)$ has degree 1, then $\overline{f}(x,y)$ will be 0.

Assume that r is a root of $f(x)$.

We will first show that if r is a repeated root of $f(x)$, then r must be a root of $f_1(x)$. To do that, we assume that r is a repeated root of $f(x)$. By definition, this means there is a polynomial $p(x)$ such that $f(x) = (x-r)^2p(x)$.

Expanding $p(x+y)$, we get

$$p(x+y) = p(x) + p_1(x)y + y^2\overline{p}(x,y)$$

Then we have

$$\begin{aligned} f(x+y) &= (x+y-r)^2 p(x+y) \\ &= [(x-r)+y]^2[p(x)+p_1(x)y+y^2\overline{p}(x,y)] \\ &= [(x-r)^2+2y(x-r)+y^2][p(x)+p_1(x)y+y^2\overline{p}(x,y)] \\ &= p(x)(x-r)^2+y[2(x-r)p(x)+p_1(x)(x-r)^2]+y^2h(x,y) \end{aligned}$$

where $h(x,y)$ is some expression in x and y. Therefore, when we expand $f(x+y)$, the sum of the terms with y^1 as their power of y is $y[2(x-r)p(x)+p_1(x)(x-r)^2]$. By definition, this sum also equals $yf_1(x)$, so $f_1(x) = 2(x-r)p(x)+p_1(x)(x-r)^2$. Substituting $x = r$ into this equation gives $f_1(r) = 2(r-r)p(r)+p_1(r)(r-r)^2 = 0$. Therefore, r is a root of $f_1(x)$.

We now assume that r is a root of both $f(x)$ and $f_1(x)$ and will deduce that $(x-r)^2$ is a factor of $f(x)$.

Since we are assuming that $f(x)$ has a root of r, we can write $f(x) = p(x)(x-r)$ for some polynomial $p(x)$. Then

$$\begin{aligned} f(x+y) &= (x+y-r)p(x+y) \\ &= [(x-r)+y][p(x)+p_1(x)y+y^2\overline{p}(x,y)] \\ &= p(x)(x-r)+y[p(x)+(x-r)p_1(x)]+y^2k(x,y) \end{aligned}$$

where $k(x,y)$ is some expression in x and y. Similar to the argument for the other direction, this implies $yf_1(x) = y[p(x)+(x-r)p_1(x)]$, hence $f_1(x) = p(x)+(x-r)p_1(x)$. We are assuming that $f_1(r) = 0$, so we can substitute $x = r$ on both sides of this equation to get $f_1(r) = p(r)+(r-r)p_1(r)$ or $0 = p(r)+0$. Therefore, $p(r) = 0$, so there is some polynomial $q(x)$ such that $p(x) = q(x)(x-r)$. Substituting into $f(x) = p(x)(x-r)$, we get $f(x) = q(x)(x-r)^2$, and so r is a repeated root of $f(x)$ by definition.

A proof using calculus. If you take a minute to verify that the polynomial $f_1(x)$ is the derivative of polynomial $f(x)$, denoted by $f'(x)$, then we can reframe this result as follows: Suppose that $f(x)$ is a polynomial and that r is a root of $f(x)$. Prove that r is a repeated root of $f(x)$ if and only if r is a root of $f'(x)$.

Assume that r is a root of $f(x)$.

Suppose that r is a repeated root of $f(x)$. Then $f(x) = p(x)(x-r)^2$ for some polynomial $p(x)$. By the product rule, $f'(x) = p'(x)(x-r)^2+2p(x)(x-r)$, so $f'(r) = p'(r)(r-r)^2+2p(r)(r-r) = 0$. Therefore, r is a root of $f'(x)$.

Now suppose that r is a root of $f'(x)$. Since r is a root of $f(x)$, there is a polynomial $p(x)$ such that $f(x) = p(x)(x-r)$. By the product rule, $f'(x) = p'(x)(x-r)+p(x)$. Substituting $x = r$ gives $f'(r) = p'(r)(r-r)+p(r)$ and since $f'(r) = 0$ by assumption, this implies $0 = 0+p(r)$, so r is a root of $p(x)$. Therefore, there is a polynomial $q(x)$ such that $p(x) = q(x)(x-r)$. Substituting gives $f(x) = p(x)(x-r) = q(x)(x-r)^2$, so r is a repeated root of $f(x)$.

(j) Suppose $p(x)$ and $q(x)$ are irreducible rational polynomials with a root, α, in common. Assume that $p(x)$ had degree n. We know that α is an algebraic number, so let $m(x)$ be its minimal polynomial.

By the division algorithm for polynomials, there are polynomials $f(x)$ and $r(x)$ such that $p(x) = f(x)m(x) + r(x)$ and the degree of $r(x)$ is *less* than the degree of $m(x)$. By the definition of the minimal polynomial, $m(\alpha) = 0$. By assumption, $p(\alpha) = 0$, so $p(\alpha) = f(\alpha)m(\alpha) + r(\alpha)$ implies that $0 = 0 + r(\alpha)$ or $r(\alpha) = 0$. Since $m(x)$ is the minimal polynomial of α and the degree of $r(x)$ is less than the degree of $m(x)$, we must have that r does not have positive degree. This means $r(x)$ is constant, and since $r(\alpha) = 0$, it must be the zero polynomial[1].

Therefore, $p(x) = f(x)m(x)$, which is a factorization of $p(x)$ into a product of two polynomials. Since $p(x)$ is irreducible and $m(x)$ has positive degree, we must have that $f(x)$ is constant. Therefore, there is a constant a such that $p(x) = am(x)$. Since $p(x)$ is irreducible, it has degree at least 1, so $a \neq 0$.

By an essentially identical argument, there is a constant $b \neq 0$ such that $q(x) = bm(x)$. Taking $c = \frac{a}{b}$, we have

$$cq(x) = cbm(x) = \frac{a}{b}bm(x) = am(x) = p(x)$$

Computing the degrees of the algebraic numbers from part (e). We can use parts (f) and (j) to prove the following: If an algebraic number is a root of an irreducible polynomial of degree d, then the degree of the algebraic number is d.

To see why this is true, suppose α is algebraic of degree d and is a root of an irreducible polynomial $p(x)$ of degree n. By part (f), the minimal polynomial, $m(x)$, of α has degree d. This means $p(x)$ and $m(x)$ are irreducible polynomials with a root, α, in common. By part (j), one is a scalar multiple of the other (and that scalar is nonzero), so they have the same degree. In other words, $n = d$.

It follows that if we are given an algebraic number α and produce an irreducible polynomial of degree d to which α is a root, we will have shown that the degree of α is d. In part (e), one can show that each of the four polynomials produced (for each algebraic number) is irreducible, so the degrees of the algebraic numbers are as stated at the end of the solution to (e).

(k) Suppose $p(x)$ is an irreducible rational polynomial with a repeated root, α. By part (h)(ii), α is also a root of $p_1(x)$. Note that if $a_n x^n$ is the leading term of $p(x)$, then $na_n x^{n-1}$ is the leading term of $p_1(x)$, and so $p_1(x)$ has degree strictly lower than that of $p(x)$. As well, $p(x)$ has a repeated root, so $n \geq 2$, which means $n - 1 \geq 1$. Therefore, $p_1(x)$ has positive degree less than n.

Every polynomial can be factored into a product of irreducible factors. To see why, we can emulate the reasoning used to see that every positive integer is the product of prime numbers. For example, if $p_1(x)$ is irreducible, then we stop. Otherwise, it can be factored as $p_1(x) = f(x)g(x)$ where each of $f(x)$ and $g(x)$ has degree at least 1 and less than that of $p_1(x)$. Now either $f(x)$ and $g(x)$ are irreducible, or they can be factored into polynomials of lower degree. Critically, the degrees always go down but stay larger than 1 when we

[1]For technical reasons, mathematicians usually distinguish the zero polynomial among the constant polynomials and do not consider it to have degree 0. Typically it is either not assigned a degree or assigned a “degree” of $-\infty$. For the purposes of this document, there is no harm in just taking the zero polynomial to have degree 0.

factor. Consequentially, this cannot go on forever, and we will eventually be left with $p_1(x)$ expressed as a product of irreducible polynomials.

Since $p_1(\alpha) = 0$, one of these irreducible factors, say $h(x)$, has α as a root. Since $h(x)$ is a factor of $p_1(x)$, its degree is no larger than the degree of $p_1(x)$, which means $h(x)$ has degree less than n.

We now have that α is a root of both $h(x)$ and $p(x)$. Both polynomials are irreducible, so part (j) implies that they must have the same degree. We have just argued that the degree of $h(x)$ is less than the degree of $p(x)$, so this is a problem.

This means our assumption that $p(x)$ has a repeated root must have been wrong, so we conclude that an irreducible rational polynomial cannot have a repeated root.