(*November 14, 2023*)

Discussion 03

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

[03.1] Find a polynomial $P \in \mathbb{Q}[x]$ so that $P(\sqrt{2}+\sqrt{3}) = 0$.

Discussion: First, we know that there *is* such a polynomial, for the general reason that algebraic extensions of algebraic extensions are still algebraic over the base field. More formulaically: let $\alpha = \sqrt{2}+\sqrt{3}$. Then

$$(\alpha - \sqrt{2})^2 \;=\; 3$$

so

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

Squaring again,

$$(\alpha^2 - 1)^2 = 4 \cdot 2 \cdot \alpha^2$$

which gives a quartic (the expected degree) for α. ///

[03.2] Find a polynomial $P \in \mathbb{Q}[x]$ so that $P(\sqrt{2}+\sqrt[3]{5}) = 0$.

Discussion: Again, there *is* such a polynomial. Let $\alpha = \sqrt{2}+\sqrt[3]{5}$. Then

$$(\alpha - \sqrt{2})^3 \;=\; 5$$

so

$$\alpha^3 + 3 \cdot 2 \cdot \alpha - 5 = (3\alpha^2 - 2)\sqrt{2}$$

Squaring gives a rational polynomial equation satisfied by α. ///

[03.3] Let α be a root of $x^2 + \sqrt{2}\,x + \sqrt{3} = 0$ in an algebraic closure of $\mathbb{Q}$. Find $P \in \mathbb{Q}[x]$ so that $P(\alpha) = 0$.

Discussion: Squaring both sides of $x^2 + \sqrt{2}x = -\sqrt{3}$ gives $x^4 + 2\sqrt{2}x^3 + 2x^2 = 3$. Rearrange to $x^4 + 2x^2 - 3 = -2\sqrt{2}x^3$, and square again, to get an octic with coefficients in $\mathbb{Q}$. ///

[03.4] Let α be a root of $x^5 - x + 1 = 0$ in an algebraic closure of $\mathbb{Q}$. Find $P \in \mathbb{Q}[x]$ so that $P(\alpha + \sqrt{2}) = 0$.

Discussion: Let $\beta = \alpha + \sqrt{2}$. Then $(\beta - \sqrt{2})^5 - (\beta - \sqrt{2}) + 1 = 0$. Expand and regroup to

$$\beta^5 + 10\beta^3 \cdot 2 + 5\beta \cdot 2 - \beta + 1 \;=\; \Big(5\beta^4 + 10\beta^2 \cdot 2 + 2 - 1\Big) \cdot \sqrt{2}$$

Square again to get a degree-ten rational equation for β. ///

[03.5] Gracefully verify that the octic $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ factors properly in $\mathbb{Q}[x]$.

Discussion: We recognize that this polynomial is $\frac{x^9-1}{x-1}$. We know that polynomials $x^n - 1$ are the products $\prod_{d|n} \Phi_d$ of cyclotomic polynomials. So $x^9 - 1 = \Phi_9(x) \cdot \Phi_3(x) \cdot \Phi_1(x)$. Thus, $\frac{x^9-1}{x-1} = \Phi_9(x) \cdot \Phi_3(x)$, a proper factorization. ///

[03.6] Gracefully verify that the quartic $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

Discussion: We recognize that that polynomial is the fifth cyclotomic polynomial, whose zeros are the primitive fifth roots of unity. A finite field $\mathbb{F}_{2^d}$ has cyclic multiplicative group, of order $2^d - 1$. Thus, there is a primitive 5^{th} root of unity ω_5 in $\mathbb{F}_{2^d}$ if and only if 5 divides $2^d - 1$. The smallest d for which this holds is $d = 4$, as $2^4 - 1 = 15$. Thus, the (necessarily irreducible) minimal polynomial for ω_5 in $\mathbb{F}_2[x]$ is of degree 4. ///

[03.7] Gracefully verify that the sextic $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_3[x]$.

Discussion: We recognize that this polynomial is the seventh cyclotomic polynomial, whose zeros are the primitive seventh roots of unity. A finite field $\mathbb{F}_{3^d}$ has cyclic multiplicative group, of order $3^d - 1$. Thus, there is a primitive 7^{th} root of unity ω_7 in $\mathbb{F}_{3^d}$ if and only if 7 divides $3^d - 1$. The smallest d for which this holds is $d = 6$, since none of $3 - 1$, $3^2 - 1$, $3^3 - 1$ is divisible by 7 (and, because $\mathbb{Z}/7^\times$ is cyclic...) we do not need to check other exponents.

Thus, the (necessarily irreducible) minimal polynomial for ω_7 in $\mathbb{F}_3[x]$ is of degree 6. ///

[03.8] Gracefully verify that the quartic $x^4 + x^3 + x^2 + x + 1$ factors into irreducible quadratics in $\mathbb{F}_{19}[x]$.

Discussion: This polynomial is the fifth cyclotomic polynomial, whose zeros are the primitive fifth roots of unity. A finite field $\mathbb{F}_{19^d}$ has cyclic multiplicative group, of order $19^d - 1$. Thus, there is a primitive 5^{th} root of unity ω_7 in $\mathbb{F}_{19^d}$ if and only if 5 divides $13^d - 1$. The smallest d for which this holds is $d = 2$.

Thus, *any* primitive fifth root of unity is (exactly) *quadratic* over $\mathbb{F}_{13}$, with quadratic minimal polynomial. Since Φ_5 has zeros (in $\overline{\mathbb{F}}_{13}$ if one wants to know *where*) exactly all the primitive fifth roots of unity, it must factor into two irreducible quadratics. ///

[03.9] Let $f(x) = x^6 - x^3 + 1$. Find primes p with each of the following behaviors: f is irreducible in $\mathbb{F}_p[x]$, f factors into irreducible quadratic factors in $\mathbb{F}_p[x]$, f factors into irreducible cubic factors in $\mathbb{F}_p[x]$, f factors into linear factors in $\mathbb{F}_p[x]$.

Discussion:

[03.10] Explain why $x^4 + 1$ properly factors in $\mathbb{F}_p[x]$ for any prime p.

Discussion: This is the eighth cyclotomic polynomial, so it has a zero in $\mathbb{F}_{p^d}$ if and only if $8|p^d - 1$. By direct observation, $p^2 = 1 \bmod 8$ for every odd p. Thus, every primitive eighth root of unity is at most quadratic over $\mathbb{F}_p$. That is, the minimal polynomials are either of degree 1 or 2, so Φ_8 factors either into four linear factors in $\mathbb{F}_p[x]$ or two (necessarily irreducible) quadratic factors in $\mathbb{F}_p[x]$. ///

[03.11] Explain why $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ properly factors in $\mathbb{F}_p[x]$ for any prime p. (*Hint:* It factors either into linear factors, irreducible quadratics, or irreducible quartics.)

Discussion: Ok, not so easy to see, but this is Φ_{15}. Thus, its zeros in an algebraic closure of $\mathbb{F}_p$ are exactly in the smallest $\mathbb{F}_{p^d}$ such that $15|p^d - 1$. By Sun-Ze, $\mathbb{Z}/15 \approx \mathbb{Z}/3 \oplus \mathbb{Z}/5$, so $\mathbb{Z}/15^\times \approx \mathbb{Z}/3^\times \oplus \mathbb{Z}/5^\times$, which is (the additive group) $\mathbb{Z}/2 \oplus \mathbb{Z}/4$. Thus, there are no elements of order 8 in $\mathbb{Z}/15^\times$, only of orders $1, 2, 4$. That is, for any prime p, either $15|p^1 - 1$ or (15 does not divide $p - 1$ and) $15|p^2 - 1$, or (15 does not divide $p^2 - 1$) and $15|p^4 - 1$. In those respective cases, Φ_{15} factors into linear, irreducible quadratics, and irreducible quartics. ///

[03.12] Why is $x^4 - 2$ irreducible in $\mathbb{F}_5[x]$?

Discussion: This is irreducible if and only if the smallest extension field $\mathbb{F}_{5^d}$ containing a fourth root of 2 is $\mathbb{F}_{5^4}$. We recall that all finite subgroups of multiplicative groups of fields are *cyclic*, so that elementary facts about cyclic groups can be invoked. Thus, in $\mathbb{F}_5^\times$, cyclic of order 4, there is only one fourth power, 1 itself, so 2 is not a fourth power there. Thus, $x^4 - 2$ has no *linear* factor in $\mathbb{F}_5[x]$. In $\mathbb{F}_{5^2}^\times$, of order $5^2 - 1 = 4 \cdot 6$, if there were α with $\alpha^4 = 2$, then

$$2^6 \;=\; (\alpha^4)^6 \;=\; \alpha^{5^2-1} \;=\; 1$$

But, computing in $\mathbb{F}_{11}$,

$$2^6 \;=\; 2^5 \cdot 2^1 \;=\; 2 \cdot 2 \;=\; 4 \;\neq\; 1 \qquad\qquad (\text{using } 2^5 = 2)$$

Thus, $x^4 - 2$ has no quadratic factors in $\mathbb{F}_5[x]$. Lacking linear or quadratic factors, it is irreducible. ///

[03.13] Why is $x^5 - 2$ irreducible in $\mathbb{F}_{11}[x]$?

Discussion: Because $\mathbb{F}_{11}^\times$ is cyclic of order 10, the only fifth powers are ± 1, so 2 is *not* a fifth power in $\mathbb{F}_{11}$, and $x^5 - 2$ has no *linear* factor in $\mathbb{F}_{11}[x]$. If there were $\alpha \in \mathbb{F}_{11^2}$ with $\alpha^5 = 2$, then

$$2^{\frac{11^2-1}{5}} \;=\; \alpha^{11^2-1} \;=\; 1$$

But, computing in $\mathbb{F}_{11}$,

$$2^{\frac{11^2-1}{5}} \;=\; 2^{12\cdot 2} \;=\; (2^1 2)^2 \;=\; 2^2 \;=\; 4 \;\neq\; 1$$

Thus, $x^5 - 2$ has no quadratic factor, either. Thus, it is irreducible in $\mathbb{F}_{11}[x]$. ///

[03.14] Let k be a field. Determine the units and ideals in the formal power series ring

$$k[[x]] \;=\; \{\sum_{n\geq 0} c_n\, x^n : \text{ arbitrary } c_n \in k\}$$

Discussion: *[... iou ...]*

[03.15] Let k be a field. Show that the field of fractions of the formal power series ring $k[[x]$ is the collection of *finite-nosed* formal Laurent series

$$k((x)) \;=\; \{\sum_{n\geq -N} c_n\, x^n : \text{arbitrary } c_n \in k,\; \text{arbitrary } N \in \mathbb{Z}\}$$

Discussion: *[... iou ...]*
