(*February 17, 2024*)

Examples 07

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

[07.1] Prove that a prime p such that $p = 1 \bmod 3$ factors *properly* as $p = ab$ in $\mathbb{Z}[\omega]$, where ω is a primitive cube root of unity. (*Hint:* If p were prime in $\mathbb{Z}[\omega]$, then $\mathbb{Z}[\omega]/p$ would be a integral domain.)

[07.2] Prove that a prime p such that $p = 2 \bmod 5$ generates a prime ideal in the ring $\mathbb{Z}[\zeta]$, where ζ is a primitive fifth root of unity.

[07.3] Find the monic irreducible polynomial with rational coefficients which has as zero

$$\alpha = \sqrt{3} + \sqrt{5}$$

[07.4] Find the monic irreducible polynomial with rational coefficients which has as zero

$$\alpha = \sqrt{3} + \sqrt[3]{5}$$

[07.5] Find the monic irreducible polynomial with rational coefficients which has as zero

$$\alpha = \frac{1 + \sqrt[3]{10} + \sqrt[3]{10}^2}{3}$$

[07.6] Let p be a prime number, and $a \in \mathbb{F}_p^\times$. Prove that $x^p - x + a$ is irreducible in $\mathbb{F}_p[x]$. (*Hint*: Verify that if α is a root of $x^p - x + a = 0$, then so is $\alpha + 1$.)

[07.7] Let $k = \mathbb{F}_p(t)$ be the field of rational expressions in an indeterminate t with coefficients in $\mathbb{F}_p$. Show that the polynomial $X^p - t \in k[X]$ is irreducible in $k[X]$, but has properly repeated factors over an algebraic closure of k.

[07.8] Let x be an indeterminate over $\mathbb{C}$. For a, b, c, d in $\mathbb{C}$ with $ad - bc \neq 0$, let

$$\sigma(x) = \sigma_{a,b,c,d}(x) = \frac{ax + b}{cx + d}$$

and define

$$\sigma\left(\frac{P(x)}{Q(x)}\right) = \frac{P(\sigma(x))}{Q(\sigma(x))}$$

for P and Q polynomials. Show that σ gives a field automorphism of the field of rational functions $\mathbb{C}(x)$ over $\mathbb{C}$.

[07.9] In the situation of the previous exercise, show that *every* automorphism of $\mathbb{C}(x)$ over $\mathbb{C}$ is of this form.

[07.10] Let s and t be indeterminates over $\mathbb{F}_p$, and let $\mathbb{F}_p(s^{1/p}, t^{1/p})$ be the field extension of the rational function field $\mathbb{F}_p(s, t)$ obtained by adjoining roots of $X^p - s = 0$ and of $X^p - t = 0$. Show that there are infinitely-many (distinct) fields intermediate between $\mathbb{F}_p(s, t)$ and $\mathbb{F}_p(s^{1/p}, t^{1/p})$.

[07.11] Fix a field k and an indeterminate t. Fix a positive integer $n > 1$ and let $t^{1/n}$ be an n^{th} root of t in an algebraic closure of the field of rational functions $k(t)$. Show that $k[t^{1/n}]$ is isomorphic to a polynomial ring in one variable.

[07.12] Fix a field k and an indeterminate t. Let $s = P(t)$ for a monic polynomial P in $k[x]$ of positive degree. Find the monic irreducible polynomial $f(x)$ in $k(s)[x]$ such that $f(t) = 0$.

[07.13] Let $p_1, p_2, \ldots$ be any ordered list of the prime numbers. Prove that $\sqrt{p_1}$ is *not* in the field

$$\mathbb{Q}(\sqrt{p_2}, \sqrt{p_3}, \ldots)$$

generated by the square roots of all the *other* primes.

[07.14] Let $p_1, \ldots, p_n$ be distinct prime numbers. Prove that

$$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_N}) = \mathbb{Q}(\sqrt{p_1} + \ldots + \sqrt{p_N})$$

[07.15] Let $\alpha = xy^2 + yz^2 + zx^2$, $\beta = x^2y + y^2z + z^2x$ and let s_1, s_2, s_3 be the elementary symmetric polynomials in x, y, z. Describe the relation between the quadratic equation satisfied by α and β over the field $\mathbb{Q}(s_1, s_2, s_3)$ and the quantity

$$\Delta^2 = (x-y)^2(y-z)^2(z-x)^2$$

[07.16] Let t be an integer. If the image of t in $\mathbb{Z}/p$ is a square for every prime p, is t necessarily a square?

[07.17] Find the irreducible factors of $x^5 - 4$ in $\mathbb{Q}[x]$. In $\mathbb{Q}(\zeta)[x]$ with a primitive fifth root of unity ζ.

[07.18] Show that $\mathbb{Q}(\sqrt{2})$ is normal over $\mathbb{Q}$.

[07.19] Show that $\mathbb{Q}(\sqrt[3]{5})$ is not normal over $\mathbb{Q}$.

[07.20] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{13})$ where ζ_{13} is a primitive 13^{th} root of unity.

[07.21] Find all fields intermediate between $\mathbb{Q}$ and a splitting field of $x^3 - x + 1$ over $\mathbb{Q}$.

[07.22] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{21})$ where ζ_{21} is a primitive 21^{st} root of unity.

[07.23] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{27})$ where ζ_{27} is a primitive 27^{th} root of unity.

[07.24] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

[07.25] Let a, b, c be independent indeterminates over a field k. Let z be a zero of the cubic

$$x^3 + ax^2 + bx + c$$

in some algebraic closure of $K = k(a, b, c)$. What is the degree $[K(z) : K]$? What is the degree of the splitting field of that cubic over K?

[07.26] Let $x_1, \ldots, x_n$ be independent indeterminates over a field k, with elementary symmetric polynomials $s_1, \ldots, s_n$. Prove that the Galois group of $k(x_1, \ldots, x_n)$ over $k(s_1, \ldots, s_n)$ is the symmetric group S_n on n things.
