University of Wyoming

Math 4520—Fall 2024

Algebra III

Fields

Department of Mathematics

Solutions to the Exam

December, 2024

1. (a) $(x+1)(x^2+2)$

   (b) $(x+1)(x^2+2)$

   (c) $(x+1)(x+\sqrt{-2})(x-\sqrt{-2})$

   (d) $(x+1)(x^2+2)$

2. The extension $F=\mathbb{Q}[\alpha]\supset\mathbb{Q}$ is normal: it contains all four roots of $m(x)$, namely

$$\begin{aligned}\alpha_1 &= 2i+\sqrt{3} = \alpha\in F,\\ \alpha_2 &= 2i-\sqrt{3} = \tfrac{1}{7}(\alpha^3+2\alpha)\in F,\\ \alpha_3 &= -2i+\sqrt{3} = -\tfrac{1}{7}(\alpha^3+2\alpha)\in F,\\ \alpha_4 &= -2i-\sqrt{3} = -\alpha\in F.\end{aligned}$$

   (a) $\{1,\alpha,\alpha^2,\alpha^3\}$. In place of the powers of α, you can substitute the corresponding powers of α_i for any of the four roots α_i. Or you can take $\{1,i,\sqrt{3},i\sqrt{3}\}$ as a basis. But clearly you cannot use $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ since these are linearly dependent.

   (b) $m(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)$.

   (c) F has exactly five subfields: $\mathbb{Q}$, $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[i\sqrt{3}]$, F. These correspond to the five subgroups of G, which are G, $\langle\tau\rangle$, $\langle\sigma\rangle$, $\langle\sigma\tau\rangle$, $\langle\iota\rangle$ respectively.

   (d) F has four automorphisms; $G=\operatorname{Aut}F=\{\iota,\sigma,\tau,\sigma\tau\}$ where

$$\begin{aligned}\iota(a+bi+c\sqrt{3}+di\sqrt{3}) &= a+bi+c\sqrt{3}+di\sqrt{3},\\ \sigma(a+bi+c\sqrt{3}+di\sqrt{3}) &= a+bi-c\sqrt{3}-di\sqrt{3},\\ \tau(a+bi+c\sqrt{3}+di\sqrt{3}) &= a-bi+c\sqrt{3}-di\sqrt{3},\\ \sigma\tau(a+bi+c\sqrt{3}+di\sqrt{3}) &= a-bi-c\sqrt{3}+di\sqrt{3}.\end{aligned}$$

   for $a,b,c,d\in\mathbb{Q}$. Note that τ is complex conjugation.

   (e) A glance at the subfields of F, listed in (c), shows that the only subfield of F containing β is F itself.

3. (a) Solve $f(x)=\phi(g(x))=g\big(\frac{1-3x}{5x-2}\big)$ for $g(x)$ gives $g(x)=\phi^{-1}(f(x))=f\big(\frac{2x+1}{5x+3}\big)$.

   (b) The subfield $\mathbb{Q}\subset F$, consisting of constant functions, is fixed by every automorphism, including ϕ.

   (c) All powers of ϕ commute. Besides ϕ and the identity, every power ϕ^k (with $k\neq 0,1$) is a valid answer. One such answer, from (a), is $\phi(f(x))=f\big(\frac{2x+1}{5x+3}\big)$. Another is $\phi^2(f(x))=\phi(\phi(f(x)))=f\big(\frac{5-14x}{25x-9}\big)$.

(d) The maps $\sigma(f(x)) = f(2x)$ and $\tau(f(x)) = f(1-x)$ are automorphisms of F. (Their inverses are $\sigma^{-1}(f(x)) = f(\frac{1}{2}x)$ and $\tau^{-1} = \tau$.) These two automorphisms do not commute since $\sigma(\tau(f(x))) = f(1-2x)$ whereas $\tau(\sigma(f(x))) = f(2-2x)$.

4. (a) *First Solution.*

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots \\ 1 &= (1-x+x^2)(a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots) \\ &= a_0 + (a_1-a_0)x + (a_2-a_1+a_0)x^2 + (a_3-a_2+a_1)x^3 + (a_4-a_3+a_2)x^3 + \cdots \end{aligned}$$

Solving for a_0=1, a_1=1, a_2=0, a_3=$-$1, etc. we have

$$f(x) = 1 + x - x^3 - x^4 + x^6 + x^7 - x^9 - x^{10} + \cdots.$$

Second Solution.

$$\begin{aligned} f(x) &= \frac{1}{1-(x-x^2)} = 1 + (x-x^2) + (x-x^2)^2 + (x-x^2)^3 + \cdots \\ &= 1 + (x-x^2) + (x^2-2x^3+x^4) + (x^3-3x^4+3x^5-x^6) + \cdots \\ &= 1 + x - x^3 + \cdots. \end{aligned}$$

(b) *First Solution.*

$$\begin{aligned} g(x) &= 1 - 2x + 3x^2 - 4x^3 + 5x^4 - 6x^5 + \cdots \\ xg(x) &= x - 2x^2 + 3x^3 - 4x^4 + 5x^5 - 6x^6 + \cdots \\ (1+x)g(x) &= 1 - x + x^2 - x^3 + x^4 - x^5 + \cdots \;=\; \frac{1}{1+x} \\ g(x) &= \frac{1}{(1+x)^2} \end{aligned}$$

Second Solution.

$$\begin{aligned} g(x) &= \frac{d}{dx}\big(x - x^2 + x^3 - x^4 + x^5 - x^6 + \cdots\big) \\ &= \frac{d}{dx}\,\frac{x}{1+x} \;=\; \frac{1}{(1+x)^2} \end{aligned}$$

5. (a) Using elementary row operations, $\left[\begin{smallmatrix} 2 & 7 \\ 11 & 4 \end{smallmatrix}\middle|\begin{smallmatrix} 5 \\ 3 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 10 \\ 11 & 4 \end{smallmatrix}\middle|\begin{smallmatrix} 9 \\ 3 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 10 \\ 0 & 11 \end{smallmatrix}\middle|\begin{smallmatrix} 9 \\ 8 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 10 \\ 0 & 1 \end{smallmatrix}\middle|\begin{smallmatrix} 9 \\ 9 \end{smallmatrix}\right]$ $\sim \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\middle|\begin{smallmatrix} 10 \\ 9 \end{smallmatrix}\right]$, giving the unique solution $(x, y) = (10, 9)$. We check to confirm that this satisfies both linear equations.

(b) The quadratic has roots $\frac{-3\pm\sqrt{3^2-4\cdot2\cdot4}}{2\cdot2} = \frac{-3\pm\sqrt{3}}{4} = \frac{-3\pm4}{4} = 9 \pm 1 = 8$ or 10.

6. (a) F (b) T (c) F (d) F (e) T (f) T (g) T (h) F (i) F (j) F

Comments (not required, but provided here for your benefit):

(a) The only automorphism of the field of real numbers is the identity map $\iota(a) = a$.

(b) This is the 'fixed field' of σ, which is featured so prominently in Galois theory.

(c) The extension $\mathbb{C} \supset \mathbb{R}$ of degree two has infinitely many one-dimensional subspaces, but only one of them, $\mathbb{R}$, is a subfield. For example, the subspace $\{bi : b \in \mathbb{R}\} \subset \mathbb{C}$ is not a subfield.

(d) The infinite field $\mathbb{F}_2(x)$ has characteristic 2.

(e) Let p be any prime divisor of n; then $n = 0$ in $\mathbb{F}_p$.

(f) In general, whenever F is a field of prime characteristic p, the map $\sigma : F \to F$, $\sigma(a) = a^p$ is a monomorphism (an injective homomorphism). When the field F is finite, this means σ is an isomorphism. So is its inverse, $\sigma^{-1}(a) = a^{1/p}$.

(g) In $F((x))$, there are uncountably many distinct elements $\sum_{i=0}^{\infty} a_i x^i$ with coefficients $a_i \in \{0, 1\}$. The same argument gives uncountably many distinct real numbers $\sum_{i=0}^{\infty} a_i 10^{-i}$ with $a_i \in \{0, 1\}$.

(h) This is a ring with zero divisors. For example, $fg = 0$ where $f(a) = \min\{0, a\}$ and $g(a) = \max\{0, a\}$.

(i) Abel's Theorem shows that this is false for a large class of polynomials of degree 5 (although the corresponding statement is true for polynomials of degree at most 4).

(j) Similarly to (h), this ring has zero divisors, e.g.

$$(1, 0, 1, 0, 1, 0, \ldots)(0, 1, 0, 1, 0, 1, \ldots) = (0, 0, 0, 0, 0, 0, \ldots).$$

However, in class we discussed how to find a maximal ideal $Z \subset \mathbb{R}^{\infty}$ such that the quotient ring $\mathbb{R}^{\infty}/Z$ is a field.