

Solution Set 10

Math 123
April 23, 2002

1. Artin §13.5 #3

- a) Note that if $f(x) = x^p - 1$ then $f'(x) = px^{p-1} = 0$, so f and f' are not relatively prime, and thus there is a field extension of F in which f has a multiple root.
- b) However, f splits in $\mathbf{F}_p \subset F$ into $f(x) = (x - 1)^p$, so it's the trivial field extension.
-
-

2. Artin §13.6 #3

By Fermat's Little Theorem, or by noting that the group of units in \mathbf{F}_{13} has order 12 and thus $3^{12} = 1$, we know that $3^{13} = 3$.

3. Artin §13.6 #7

First note that, as above, $a^3 = a$ for each $a \in \mathbf{F}_3$. Thus $x^9 - x$ will have 0, 1 and 2 as roots. Dividing out, we find that

$$\frac{x^9 - x}{x(x-1)(x-2)} = (x^2 + 1)(x^4 + 1).$$

The first factor is irreducible since $(\pm 1)^2 = 1$. Similarly, the second has no linear factor, but it factors into

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

Thus $x^9 - x = x(x^2 + 1)(x^2 + x - 1)(x^2 + x + 1)$.

As was computed in the second problem set, we know all of the irreducible polynomials of degree 3 over \mathbf{F}_3 ; by Artin 6.4(e), we can thus write

$$\begin{aligned} x^{27} - x &= (x^3 - x + x^3 - x - 1)(x^3 + x^2 - 1)(x^3 + x^3 + x - 1)(x^3 - x^2 - x - 1) \\ &\quad (x^3 + x^2 - x + 1)(x^3 - x^2 + 1)(x^3 - x^2 + x + 1). \end{aligned}$$

4. Artin §13.6 #10

Since the polynomial $x^2 - 1$ has exactly two roots ± 1 in any field of characteristic not 2, we know that $a^{-1} \neq a$ for all $a \in K^*$, $a \neq \pm 1$. Thus

$$\prod_{K^*} a = 1 \cdot (-1) \cdot (a_1 a_1^{-1})(a_2 a_2^{-1}) \cdots (a_n a_n^{-1}) = -1.$$

If K has characteristic 2 then the above product will be $1 = -1$.

5. Artin §13.6 #11

Again by Fermat's Little Theorem, we know that $a^p = a$ for any $a \in \mathbf{F}_p$. Thus $x^p - a = (x - a)^p$, i.e. $x^p - a$ has exactly one root.

6. Artin §13.6 #15

Let $a \in K$ be a root of f , so $a^3 + a + 1 = 0$. Thus

$$(a + 1)^3 + (a + 1)^2 + 1 = (a^3 + a^2 + a + 1) + (a^2 + 1) + 1 = a^3 + a + 1 = 0$$

so $a + 1$ is a root of g . Thus L embeds into K , i.e. $L \cong \mathbf{F}_2/(g) \cong \mathbf{F}_2(a + 1) \subset K$, and since $|L| = |K| = 8$ (since f and g are both irreducible cubics), we must have $L \cong K$. Explicitly, this isomorphism sends $a + 1$ to b , where a is a root of f in K and b is a root of g in L (and since a and b generate K and L , respectively, this is enough to determine the image of any element).

7. Artin §13.7 #6

- a) By Artin Theorem 7.14 and Corollary 7.15, the number of isomorphism classes of degree 3 field extensions K of $F = \mathbf{C}(x)$ that ramify at ± 1 is the same as the number of isomorphism classes of connected 3-sheeted branched coverings of F that branch at ± 1 . Since we can construct any such branched covering by cutting and pasting three copies of \mathbf{C} , we need only solve the next part.
- b) Cut \mathbf{C} along $(-\infty, -1]$ and $[1, \infty)$. The cover is thus completely determined by the permutations σ_1 and σ_{-1} of the sheets obtained by going around the points $+1$ and -1 , respectively, in a counter-clockwise direction; by Proposition 7.18, two such covers are isomorphic if and only if the associated permutations are conjugate. Note that conjugating a permutation is the same as acting the permutation on a different labeling of the sheets.

Let $\rho = (123)$, $\tau_1 = (23)$, $\tau_2 = (13)$, and $\tau_3 = (12)$, so $S_3 = \{1, \rho, \rho^2, \tau_1, \tau_2, \tau_3\}$. We can simply try all combinations of $\sigma_{\pm 1}$ to obtain the following five isomorphism (conjugacy) classes of (σ_1, σ_{-1}) :

- (ρ, ρ) represents the class where $\sigma_{\pm 1}$ are the same 3-cycle.
- (ρ, ρ^2) represents the class with $\sigma_{\pm 1}$ different (i.e. opposite) 3-cycles.
- (ρ, τ_1) represents the class with σ_1 a 3-cycle and σ_{-1} a transposition

- (τ_1, ρ) represents the class with σ_1 a transposition and σ_{-1} a 3-cycle.
- (τ_1, τ_3) represents the class where $\sigma_{\pm 1}$ are different transpositions.

There are no more cases to consider, as follows. First of all, neither of $\sigma_{\pm 1}$ can be the identity, because then the cover would not branch at one point. Also, $\sigma_{\pm 1}$ cannot be the same transposition because then the cover would not be connected.

- c) We find the polynomials $f(x, y)$ in the same order as above. A note on proving irreducibility: using Artin's general Theorem 3.3.9 and Proposition 3.4.7, we can apply most of the machinery for proving irreducibility of integer polynomials to the ring $\mathbf{C}[x]$, which has field of fractions $\mathbf{C}(x)$. Note also that in order to prove that f ramifies exactly at ± 1 , one can find the roots of $\partial f / \partial y$ and solve for the values of x such that $f(x, y) = 0$ as well.

- $f(x, y) = y^3 - (x+1)(x-1)$, i.e. we would like to say $y(x) = \sqrt[3]{x+1}\sqrt[3]{x-1}$. This has triple roots at $x = \pm 1$ (since $\partial f / \partial y = 3y^2 = 0 \iff y = 0 \iff x = \pm 1$) and is irreducible by Eisenstein's criterion (with prime $x+1$); thus its Riemann surface is isomorphic to one of the first two cases above. Now, if x is very large then $y(x)$ will be approximately $x^{2/3}$, so going counter-clockwise around a circle of very large radius will increase the argument of y by $2\pi \cdot 2/3 = 4\pi/3$, so y will be different after going around this loop. But in the second case above, starting with x far from the origin on the negative imaginary axis and going around a circle centered at the origin in a counter-clockwise direction will bring you back to where you started (you go down one sheet and then back up), so $f(x, y)$ must have a Riemann surface isomorphic to the one in the first case.
- $f(x, y) = y^3 - (x+1)^2(x-1)$. Similarly to above, this has triple roots at $x = \pm 1$ and is irreducible by Eisenstein (with prime $x-1$). However, now $y(x) \approx x$ for large x , so following a large circle around the origin in a counter-clockwise direction will not change the argument of y , so you will end up in the same place you started. Thus the Riemann surface for f is indeed that of the second case.
- $f(x, y) = (x-1)y^3 - 3(x-1)y + 2(x+3)$. The analysis in this case is a bit more difficult. We have $\partial f / \partial y = 3(x-1)(y^2 - 1)$, which is zero when $y = \pm 1$ or $x = 1$. The case $y = 1$ gives no solution for x , while $y = -1$ implies $x = -1$, which gives $f(-1, y) = -2y^3 + 6y + 4 = -2(y-2)(y+1)^2$ which has a double root. When $x = 1$, there is no solution for y ; however, we can rewrite our equation as

$$x = \frac{y^3 - 3y - 6}{y^3 - 3y + 2}.$$

Now, when $x = 1$, this can be written as $0 = -8/(y^3 - 3y + 2)$, which has a triple root as $y \rightarrow \infty$ — that is, as $x \rightarrow 1$, all three sheets of the Riemann surface converge, so although there is no point $(1, \infty)$ on the Riemann surface, if we fill in the puncture (remember $\mathbf{C}[x, y]/(f)$ is the field of continuous functions on a branched cover minus a finite set of points), we obtain a branched cover that ramifies with a triple root at 1 and a double root at -1 , which is indeed the cover in the third case.¹

¹You might now object that $y = 1$ above *does* give a solution for x , namely $x = \infty$. This is true, but we are not considering ∞ to be a point of ramification.

- $f(x, y) = (x + 1)y^3 - 3(x + 1)y^2 + 2(x - 3)$. This situation is analogous to the previous one.
- $f(x, y) = y^3 - 3y - 2x$. We have $\partial f / \partial y = 3(y^2 - 1) = 0 \iff y = \pm 1 \iff x = \pm 1$, so f ramifies at $x = \pm 1$; indeed, $f(\pm 1, y) = (y - 2)(y \pm 1)^2$, so f has a double root at ± 1 . Thus if f is irreducible then it must have the Riemann surface of case five. We can use the rational root theorem to check irreducibility—since f is monic and cubic in y , we need only check whether a constant or a constant times x satisfies f . This is clearly seen not to be the case by keeping track of the highest degree of x .

If you didn't get the polynomials in the third and fourth case, don't feel bad—nobody did,² and I didn't take off points.

8. Artin §13.8 #1

If α is algebraic over F then α satisfies some polynomial $f \in F[x]$, so since $f \in F(\beta)[x]$, we know that α is algebraic over $F(\beta)$. If α is transcendental over F then $\{\beta\}$ is a transcendence basis for K over F , so by definition, α is algebraic over $F(\beta)$.³

9. Artin §13.8 #2

Let $\varphi : \mathbf{Q}(\pi) \rightarrow \mathbf{Q}(e)$ be the isomorphism taking $\pi \mapsto e$. We will show that φ cannot be extended to a continuous function $\mathbf{R} \rightarrow \mathbf{R}$ (the subspace topology of the countable set $\mathbf{Q}(\pi) \subset \mathbf{R}$ is the discrete topology!). Let $x_n \in \mathbf{Q}$ be a sequence that converges to π , i.e. $\lim_{n \rightarrow \infty} x_n = \pi$. We have $\varphi(x_n) = x_n$ since φ fixes \mathbf{Q} , but $\lim_{n \rightarrow \infty} \varphi(x_n) = \pi$ and $\varphi(\lim_{n \rightarrow \infty} x_n) = e$.

Joe Rabinoff

²Including me.

³Recall that we gave an elementary proof of this in section.