D-MATH
Prof. Richard Pink

Solutions 14

Hyperelliptic Curves, Coverings

1. Let k be a perfect field of characteristic $p > 0$.

   (a) Let K be a finitely generated field extension of k of transcendence degree 1. Prove that for any $r \geqslant 1$ the only purely inseparable extension of degree p^r of K is the overfield $\{x^{1/p^r} \mid x \in K\}$.

   (b) Deduce that for every purely inseparable finite morphism of curves $X \to Y$ over k we have $g(X) = g(Y)$.

   Solution: (a) By induction on r the problem reduces to the case $r = 1$. Let $L := \{x^{1/p} \mid x \in K\}$ within an algebraic closure of K; this is a purely inseparable extension of K. Any inseparable extension E/K of degree p is generated by an element of the form $a^{1/p}$ for some $a \in K$ and hence contained in L. It therefore suffices to prove that $[L/K] = p$.

   For this choose $t \in K$ transcendental over k such that $[K/k(t)]$ is minimal. Then $t^{1/p} \in L \smallsetminus K$, and so $K(t^{1/p})/K$ is a subextension of L/K of degree p. It therefore suffices to show that $L = K(t^{1/p})$.

   For this consider any $a \in K$. We compare the degrees of the following finite field extensions within L:

$$\begin{tikzcd}[arrows=dash]
& k(t^{1/p}, a^{1/p}) \arrow[d] \arrow[dd, bend left=60] \\
& k(t^{1/p}, a) \arrow[dl, "p"'] \arrow[d] \\
k(t, a) \arrow[d] & k(t^{1/p}) \arrow[dl, "p"] \\
k(t) &
\end{tikzcd}$$

   On the one hand we have $t^{1/p} \notin K$ and so $t^{1/p} \notin k(t,a)$; hence $k(t^{1/p}, a)/k(t,a)$ is inseparable of degree p, just as $k(t^{1/p})/k(t)$. On the other hand, since k is perfect, the Frobenius homomorphism $x \mapsto x^p$ induces a commutative diagram with horizontal isomorphisms

$$\begin{tikzcd}
k(t^{1/p}, a^{1/p}) \arrow[r, "(\ )^p", "\sim"'] & k(t,a) \\
k(t^{1/p}) \arrow[u, hook] \arrow[r, "(\ )^p", "\sim"'] & k(t). \arrow[u, hook]
\end{tikzcd}$$

Thus $\big[k(t^{1/p}, a^{1/p})/k(t^{1/p})\big] = \big[k(t,a)/k(t)\big]$. The multiplicativity of degrees in field extensions therefore implies that

$$\big[k(t^{1/p}, a^{1/p})/k(t)\big] = \big[k(t^{1/p}, a)/k(t)\big].$$

Thus $k(t^{1/p}, a^{1/p}) = k(t^{1/p}, a)$ and hence $a^{1/p} \in k(t^{1/p}, a) \subset K(t^{1/p})$. Since a was arbitrary, it follows that $L \subset K(t^{1/p})$ and hence $L = K(t^{1/p})$, as desired.

(b) If $X \to Y$ is purely inseparable and finite, the corresponding field extension $K(X)/K(Y)$ is purely inseparable of degree p^r for some $r \in \mathbb{Z}_{\geqslant 0}$. By (a) we therefore have $K(X)^{p^r} = K(Y)$ and hence the following commutative diagram

$$\begin{tikzcd}
K(Y) & K(X) \arrow[l, "\sim"', "(\ )^{p^r}"] \\
k \arrow[u, hook] & k. \arrow[l, "\sim"', "(\ )^{p^r}"] \arrow[u, hook]
\end{tikzcd}$$

Because $K(Y)$ is the pushout of this diagram, we obtain an isomorphism $f : K(X) \otimes_{k,(\ )^{p^r}} k \xrightarrow{\sim} K(Y)$. Let $\mathrm{Frob}_{p^r} : \operatorname{Spec} k \to \operatorname{Spec} k$ be the automorphism induced by the Frobenius $(\ )^{p^r} : k \xrightarrow{\sim} k$. Then f corresponds to an isomorphism of curves $Y \xrightarrow{\sim} X \times_{\operatorname{Spec} k, \mathrm{Frob}_{p^r}} \operatorname{Spec} k$. Thus $g(X) = g(Y)$ as the genus is stable under flat base change.

Caution: The fields $K(X)$ and $K(Y)$ are not necessarily isomorphic as field extensions of k. Their isomorphy as abstract fields does not yet prove (b), because the genus is an invariant of a curve or of its function field *over* k.

2. Let k be an algebraically closed field of characteristic 2 and let $g \geqslant 1$. Show that the smooth projective curve with the affine equation

$$y^2 + y = x^{2g+1}$$

is hyperelliptic of genus g. Hence there exist hyperelliptic curves of every genus $\geqslant 1$ in characteristic 2.

Solution: Set $a(x,y) := y^2 + y - x^{2g+1}$. Since $\frac{\partial a}{\partial y} = 1$, the chart $U := \operatorname{Spec} k[x,y]/(a)$ is nonsingular by the jacobian criterion. Next substitute $x = s^{-1}$ and $y = s^{-g-1}t$, which transforms the equation into $b(s,t) := t^2 + s^{g+1}t - s = 0$. Here $\frac{\partial b}{\partial t} = s^{g+1}$ is zero if and only if s is zero, in which case $\frac{\partial b}{\partial s} = (g+1)s^g t - 1$ is non-zero. Thus the chart $V := \operatorname{Spec} k[s,t]/(b)$ is also nonsingular by the jacobian criterion. The morphisms $U \to \mathbb{P}^1_k$, $(x,y) \mapsto [x:1]$ and $V \to \mathbb{P}^1_k$, $(s,t) \mapsto [1:s]$ glue to a finite separable morphism $f\colon U \cup V \to \mathbb{P}^1_k$ of degree 2. Thus $U \cup V$ is the desired smooth projective curve X. To determine the genus of X note that

$$\begin{aligned} k[x,y]/(a) &= k[x] \oplus k[x]\cdot y \quad \text{and} \\ k[s,t]/(b) &= k[s] \oplus k[s]\cdot t \;=\; k[x^{-1}] \oplus k[x^{-1}]\cdot x^{-g-1}y. \end{aligned}$$

Together this shows that

$$f_*\mathcal{O}_X \;=\; \mathcal{O}_{\mathbb{P}^1_k} \oplus \mathcal{O}_{\mathbb{P}^1_k}(-(g+1)\infty)\cdot y.$$

Thus X has genus

$$h^1(X,\mathcal{O}_X) = h^1(\mathbb{P}^1_k, f_*\mathcal{O}_X) = h^1(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1_k}) + h^1(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1_k}(-(g+1)\infty)) = 0 + g = g.$$

3. Let $F \in k[x]$ be a separable polynomial of even degree $\geqslant 2$ over an algebraically closed field k with $\operatorname{char} k \neq 2$. Let X be the smooth projective curve over k with the affine equation $y^2 = F(x)$ and let $R := k[x,y]/(y^2 - F(x))$. Show that the following properties are equivalent:

   (a) There exist $A, B \in k[x]$ with $B \neq 0$ such that $A^2 - FB^2 = 1$.

   (b) $R^\times \neq k^\times$.

   (c) Let $P_1, P_2 \in X$ be the two points at infinity where x has a pole. Then the divisor class $[P_1 - P_2] \in \mathrm{Cl}^0(X)$ is an element of finite order.

   **Give examples where these properties hold and where they don't.

   Solution: Note that $R = k[x] \oplus y\cdot k[x]$, and the hyperelliptic involution is the automorphism $\sigma\colon (x,y) \mapsto (x,-y)$. By the course there are precisely two points of X above the point $x = \infty$ of $\mathbb{P}^1_k$, and they are interchanged by σ.

   (a)$\Rightarrow$(b): Consider $A, B \in k[x]$ with $B \neq 0$ such that $A^2 - FB^2 = 1$. Then in R we have $(A+yB)(A-yB) = 1$. But that means that $A + yB \in R \smallsetminus k$ has the inverse $A - yB$, proving (b).

   (b)$\Rightarrow$(a): Consider $A, B \in k[x]$ such that $A + yB$ is a unit in R but not in $k^\times$, say with inverse $A' + yB'$ for $A', B' \in k[x]$. Applying σ we find that $A - yB$ is also a unit with inverse $A' - yB'$. Taking products it follows that $A^2 - FB^2$ is a unit with inverse $A'^2 - FB'^2$. But these are now elements of $k[x]$, whose group of units is $k^\times$; hence $A^2 - FB^2 \in k^\times$. Since k is algebraically closed, we can write $A^2 - FB^2 = a^2$ for some $a \in k^\times$. After replacing (A,B) by $(A/a, B/a)$ we get $A^2 - FB^2 = 1$. Finally, if $B = 0$, we get $AA' = 1$ with $A, A' \in k[x]$, so that $A + yB = A \in k[x]^\times = k^\times$, contrary to the assumption. Thus A, B satisfy (a).

(b)⇒(c): Consider any $f \in R^\times \smallsetminus k^\times$. Then the divisor of f is non-zero and trivial on $\operatorname{Spec} R$. Thus $\operatorname{div}(f) = n_1 P_1 + n_2 P_2$ for some integers n_1, n_2 which are not both zero. Since any principal divisor has total degree 0, we must then in fact have $\operatorname{div}(f) = n(P_1 - P_2)$ for some non-zero integer n. But that means that $|n|$ times that divisor class $[P_1 - P_2]$ is the trivial divisor class.

(c)⇒(b): Suppose that $n[P_1 - P_2] = 0$ in $\mathrm{Cl}^0(X)$ for some integer $n > 0$. Then $n(P_1 - P_2) = \operatorname{div}(f)$ for some non-zero $f \in K(X)$. This f then has no poles or zeros in the chart $\operatorname{Spec} R$; so both it and its inverse lie in R and hence in $R^\times$. Since $\operatorname{div}(f) \neq 0$, we also have $f \notin k^\times$ and hence $f \in R^\times \smallsetminus k^\times$.

Constructing examples for both cases is not so easy. If k is the algebraic closure of a finite field $\mathbb{F}_q$ and F has coefficients in $\mathbb{F}_q$, the divisor class $[P_1 - P_2]$ always has finite order. The reason is that $\mathrm{Cl}^0(X) \cong J(k)$ where J is the jacobian variety of X, and the class $[P_1 - P_2]$ corresponds to a point in the finite subgroup $J(\mathbb{F}_q)$. But the way that the order of $[P_1 - P_2]$ depends on the coefficients of F is very complicated.

With some knowledge of elliptic curves one can construct examples for both cases with $g = 1$. Namely, take any curve E of genus 1 over k and any closed point P_0. Then we have a bijection $|E| \to \mathrm{Cl}^0(X)$, $P \mapsto [P - P_0]$. By solving some explicit equations one can always produce a point $P \neq P_0$ such that $[P - P_0]$ has finite order. By contrast, for most points that one writes down randomly one can prove that $[P - P_0]$ does not have finite order. In either case one then writes E as a double cover of $\mathbb{P}^1_k$ such that P_0 and P are precisely the two points above ∞ (compare the solution to problem 4a below), so that $(E, P, P_0) = (X, P_1, P_2)$ has the desired property.

4. Let k be an algebraically closed field of characteristic $\neq 2$. An *elliptic curve* is an irreducible smooth projective curve of genus 1. Prove:

   (a) Show that for any two distinct closed points P and Q on an elliptic curve E there exists an automorphism $\sigma\colon E \to E$ of order 2 with $\sigma(P) = Q$.

   (b) For any $\lambda \in k \smallsetminus \{0, 1\}$ the curve $E_\lambda \subset \mathbb{P}^2_k$ that is given by the equation
   $$ZY^2 = X(X - Z)(X - \lambda Z)$$
   is an elliptic cuve.

   (c) Show that any elliptic curve E is isomorphic to some such E_λ.

   (d) Show that $E_\lambda \cong E_\mu$ if and only if
   $$\mu \in \left\{\lambda, \tfrac{1}{\lambda}, 1 - \lambda, \tfrac{1}{1-\lambda}, \tfrac{\lambda}{\lambda-1}, \tfrac{\lambda-1}{\lambda}\right\}.$$

   (e) The *j-invariant* of an elliptic curve E is the element
   $$j(E) := 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \in k$$

for any $\lambda \in k$ with $E_\lambda \cong E$. Show that $E \mapsto j(E)$ induces a bijection from the set of isomorphism classes of elliptic curves over k to k.

Solution: (a) This solution partly follows the proof of Lemma IV.4.2 in Hartshorne. Consider the divisor $D := P + Q$. Then $h^1(X, \mathcal{O}_X(D)) = 0$, because $\deg D = 2 > 2g(E) - 2 = 0$. Hence $h^0(X, \mathcal{O}_X(D)) = \deg D = 2$, and so D induces a morphism $f : E \to \mathbb{P}^1_k$ of degree 2 with $f^*\infty = D$. This morphism is separable, because the characteristic is not 2. Therefore $K(E)$ is Galois of degree 2 over $K(\mathbb{P}^1_k) = k(x)$. The induced involution $\sigma \in \mathrm{Gal}(K(E)/k(x))$ then acts on X over $\mathbb{P}^1_k$ and interchanges P and Q.

(b) Same calculation as for general hyperelliptic curves in the course.

(c) Pick a closed point $P \in E$ and repeat the construction in (a) with the divisor $D := 2P$. This yields a separable morphism $f : E \to \mathbb{P}^1_k$ of degree 2 with $f^*\infty = 2P$. By the general formula for hyperelliptic curves from the course the curve E is then given by an affine equation of the form $y^2 = c(x)$ for a separable polynomial $c \in k[x]$ of degree 3. After a linear substitution of the form $x \rightsquigarrow \alpha x + \beta$ we may suppose that c has the roots 0 and 1. After another substitution $y \rightsquigarrow \gamma y$ this yields the equation $y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in k \setminus \{0, 1\}$. Thus $E \cong E_\lambda$.

(d) As for any hyperelliptic curve, for any elliptic curve E the morphism $E \to \mathbb{P}^1_k$ of degree 2 is unique up to an automorphism of $\mathbb{P}^1_k$. Thus the set of 4 branch points in $\mathbb{P}^1_k$ is unique up to $\mathrm{Aut}(\mathbb{P}^1_k)$. For E_λ this is the set $\{0, 1, \lambda, \infty\}$. Thus we must show that there exists $\varphi \in \mathrm{Aut}(\mathbb{P}^1_k)$ with $\varphi(\{0, 1, \lambda, \infty\}) = \{0, 1, \mu, \infty\}$ if and only if μ lies in the indicated set. Any such φ must map the points to each other in one of $|S_4| = 24$ different ways. Recall that $\mathrm{Aut}(\mathbb{P}^1_k) \cong \mathrm{PGL}_2(k)$ via Möbius transformations, and that any Möbius transformation is determined by the images of three distinct points. Thus each case reduces to a quick finite computation. The total calculation can be sped up a lot by exploiting the fact that the possibilities for μ are obtained from the Möbius transformations

$$t \mapsto t,\ \frac{1}{t},\ 1-t,\ \frac{1}{1-t},\ \frac{t}{t-1},\ \frac{t-1}{t}$$

which form a subgroup $G < \mathrm{Aut}(\mathbb{P}^1_k)$ that is isomorphic to S_3.

(e) The group G acts faithfully on the rational function field $k(t)$; hence $k(t)/k(t)^G$ is a finite Galois extension with Galois group G. Direct computation shows that the rational function

$$j(t) := 2^8 \cdot \frac{(t^2 - t + 1)^3}{t^2(t-1)^2}$$

is G-invariant. The degree of the extension $k(t)/k(j)$ is the maximum of the degrees of the numerator and the denominator of j, which is 6. Since $|G| = 6$, we deduce that $k(t)^G = k(j)$. Thus j corresponds to separable morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$ of degree 6. As the associated field extension is Galois, the Galois group acts transitively on all fibers by the same argument as in the last lecture. Thus j induces an injective map

$$(k \smallsetminus \{0,1\})/G \hookrightarrow k,\ [\lambda] \mapsto j(\lambda).$$

To show that this is surjective, consider any $j_0 \in k$. Since k is algebraically closed of characteristic $\neq 2$, the equation $2^8(t^2-t+1)^3 - t^2(t-1)^2 j_0 = 0$ has a solution $\lambda \in k$. This solution cannot be 0 or 1; hence $j(\lambda) = j_0$. The map is therefore surjective and hence bijective. Finally, (c) and (d) imply that the isomorphism classes of elliptic curves over k are in bijection with the set $(k \smallsetminus \{0,1\})/G$, so (e) follows.

5. Show that the hyperelliptic curve over $\mathbb{C}$ with the affine equation $y^2 = x^5 - x$ has precisely 48 automorphisms.

   Solution: Denote the curve by X and consider the morphism $f : X \to \mathbb{P}^1_{\mathbb{C}}$, $(x,y) \mapsto x$ of degree 2. Since composition with automorphisms of $\mathbb{P}^1_{\mathbb{C}}$ yields all morphisms $X \to \mathbb{P}^1_{\mathbb{C}}$ of degree 2, the group $\mathrm{Aut}_k(X)$ acts on the ramification points of f. Let $P_1, \ldots, P_4, Q_1, Q_2$ be the ramification points over $1, i, -1, -i, 0, \infty \in \mathbb{P}^1_{\mathbb{C}}$, respectively. The automorphisms defined as

$$\begin{aligned}(x,y) &\mapsto (ix, y)\\ (x,y) &\mapsto (1/x, iy/x^3)\end{aligned}$$

   act on $\{P_1, \ldots, P_4\}$ as the dihedral group D_4 of order 8. The automorphism defined as

$$(x,y) \mapsto \left(\tfrac{-ix+1}{x+1}, \tfrac{y}{(-i)^{1/2}(x+1)^3}\right),$$

   with any choice of $(-i)^{1/2}$ has order 3 and acts nontrivially on the ramification points. Furthermore the hyperelliptic involution acts on X and fixes all ramification points. One checks that these automorphisms generate a subgroup of $\mathrm{Aut}_k(X)$ of order 48.

   On the other hand, as a hyperelliptic curve with 6 ramification points, X is a curve of genus 2. By Hurwitz we thus have $|\,\mathrm{Aut}(X)| \leqslant 84(2-1) = 84$. Since $\mathrm{Aut}(X)$ already contains a subgroup of order 48 with $2 \cdot 48 = 96 > 84$, we conclude that $|\,\mathrm{Aut}(X)| = 48$.

6. Let k be an algebraically closed field of characteristic $p \geqslant 5$ and consider the hyperelliptic curve X of genus g given by

$$y^2 = x^p - x.$$

   Show that $|\,\mathrm{Aut}(X)| \geqslant 2p(p^2-1) > 16g^3$.

Solution: Consider the automorphisms

$$
\begin{aligned}
&(x,y) \mapsto (x+1, y), \\
&(x,y) \mapsto (\alpha x, \sqrt{\alpha}\, y) \qquad \text{for any } \alpha \in \mathbb{F}_p^\times \text{ and any square root in } k^\times, \\
&(x,y) \mapsto \Big(-1/x, \frac{y}{x^{(p+1)/2}}\Big).
\end{aligned}
$$

They act on the x-coordinate through the Möbius transformations associated to the respective matrices

$$
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
$$

By a well-known exercise from Algebra I these matrices generate the group $\mathrm{GL}_2(\mathbb{F}_p)$. Since $\mathrm{PGL}_2(\mathbb{F}_p) = \mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times$, we deduce that $|\,\mathrm{PGL}_2(\mathbb{F}_p)| = |\,\mathrm{GL}_2(\mathbb{F}_p)|/|\mathbb{F}_p^\times| = (p^2-1)(p^2-p)/(p-1) = p(p^2-1)$. In addition the hyperelliptic involution $(x,y) \mapsto (x,-y)$ acts trivially on the x-coordinate. Thus $|\,\mathrm{Aut}(X)| \geqslant 2p(p^2-1)$. On the other hand, since p is odd, by the course we have $p+1 = 2g+2$. Thus $2p(p^2-1) > 16g^3$.