Algebraic Geometry
D-MATH, FS 2016

Prof. Pandharipande

Exercise Sheet 3 - Solutions

1. Prove the following basic facts about algebraic maps.

a) For $f : X \to Y$ and $g : Y \to Z$ algebraic morphisms of quasi-projective varieties, the composition $g \circ f : X \to Z$ is algebraic.

b) For affine varieties $V \subset \mathbb{C}^n$, $W \subset \mathbb{C}^m$, the algebraic maps $V \to W$ are exactly given by

$$f : V \to \mathbb{C}^m, v \mapsto (f_1(v), \ldots, f_m(v)),$$

where $f_1, \ldots, f_m \in \Gamma(V)$ are algebraic functions on V such that the image of the map f above is contained in W.

c) For quasi-projective varieties X, Y and a cover $X = \bigcup_{i \in I} V_i$ of X with open subsets V_i, a map $\varphi : X \to Y$ is algebraic if and only if the restriction $\varphi|_{V_i}$ is algebraic for all $i \in I$. In particular, for an open cover $Y = \bigcup_{i \in I} W_i$ it suffices to check that $\varphi^{-1}(W_i)$ is open in X and that

$$\varphi|_{\varphi^{-1}(W_i)} : \varphi^{-1}(W_i) \to W_i$$

is algebraic for all $i \in I$.

d) Show that the statement in b) remains true if V is a quasi-projective variety.

e) If $X \subset \mathbb{P}^n$ is a quasi-projective variety and if $F_0, \ldots, F_m \in \mathbb{C}[Z_0, \ldots, Z_m]$ are homogeneous polynomials of the same degree, which do not have a common zero on X, then

$$F : X \to \mathbb{P}^m, \xi \mapsto [F_0(\xi), \ldots, F_m(\xi)]$$

defines an algebraic morphism.

Solution

a) The map $g \circ f$ is continuous with respect to the Zariski topology as the composition of two continuous functions. For $W \subset Z$ open and $h : W \to \mathbb{C}$ algebraic, we have that $h \circ g : g^{-1}(W) \to \mathbb{C}$ is algebraic because g is algebraic and then $h \circ g \circ f : f^{-1}(g^{-1}(W)) \to \mathbb{C}$ is algebraic as f is algebraic.

b) First for $f_1, \ldots, f_m \in \Gamma(V)$ such that $f = (f_1, \ldots, f_m)$ has image in W, the map f is algebraic. Indeed, for $W' \subset W$ a closed set cut out by polynomials $g_1, \ldots, g_r \in \mathbb{C}[y_1, \ldots, y_m]$, the set $f^{-1}(W')$ is cut out in V by the equations

$$g_i(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) = 0 \text{ for } i = 1, \ldots, r.$$

As all g_i and f_j are given by polynomials (recall $\Gamma(V) = \mathbb{C}[x_1, \ldots, x_n]/I(V)$), these equations are again polynomials, so indeed $f^{-1}(W')$ is a closed set.
On the other hand let $S \subset W$ be open and $h : S \to \mathbb{C}$ be algebraic. Then locally, h is given as the quotient $h = g_1/g_2$ for two polynomials g_1, g_2. But then $h \circ f$ is locally given as the quotient of the polynomials $g_1(f_1, \ldots, f_m)$ and $g_2(f_1, \ldots, f_m)$, so it is again algebraic.
Now assume conversely that $f : V \to W$ is algebraic. Then as the functions $y_1, \ldots, y_m : W \to \mathbb{C}$ are algebraic, the compositions $f_1 = y_1 \circ f, \ldots, f_m = y_m \circ f$ are all algebraic functions on V, hence contained in $\Gamma(V)$. But then $f = (f_1, \ldots, f_m)$ is of the claimed form, finishing the proof.

c) First we note that the inclusions $V_i \to X$ are algebraic. Indeed, the V_i carry the subset topology from the Zariski topology on X and for an algebraic function on some open set $W \subset X$, its restriction to $V_i \cap W$ is still algebraic. Hence one direction of the statement above is clear: if φ is algebraic, we know $\varphi|_{V_i}$ is just the composition of the inclusion $V_i \to X$ with the map φ and so it is again algebraic.
On the other hand let all the $\varphi|_{V_i}$ be algebraic. Then, as continuity of a function can be checked on an open cover of the domain, the function φ is continuous. On the other hand, for any algebraic function h on an open subset $W \subset Y$, the function $h \circ \varphi$ defined on $\varphi^{-1}(W)$ is algebraic on all open sets $\varphi^{-1}(W) \cap V_i$ by assumption, and these sets cover $\varphi^{-1}(W)$. But the definition of an algebraic function can be checked locally, so indeed $h \circ \varphi$ is algebraic.

d) Let $V = \bigcup_{i \in I} V_i$ be a cover of V by affine varieties V_i. Then a map $f = (f_1, \ldots, f_n) : V \to W$ is algebraic iff $f|_{V_i}$ is algebraic for all $i \in I$. But now we are in the situation of b), so $f|_{V_i}$ is algebraic iff all component functions $f_j|_{V_i}$ are algebraic. Again using the last exercise part, this is the case iff the functions f_j are algebraic, which finishes the proof.

e) One verifies immediately that the fact that all F_i have the same degree implies that F is well-defined, that is independent of the representative $\xi \in \mathbb{C}^{n+1} \setminus \{0\}$ of $[\xi] \in X \subset \mathbb{P}^n$. By the previous exercise, we may check that F is algebraic on the preimages of an open cover of $\mathbb{P}^m$. Let us choose the standard open cover $\mathbb{P}^m = \bigcup_{i=0}^m U_i$ with $U_i = \{[x_0, \ldots, x_m] : x_i \neq 0\} \cong \mathbb{C}^m$. We have $F^{-1}(U_i) = X \setminus V(F_i)$ is indeed an open set and here we have

$$\begin{array}{ccccc} F : F^{-1}(U_i) & \to & U_i & \xrightarrow{\sim} & \mathbb{C}^n \\ [\xi] & \mapsto & [F_0(\xi), \ldots, F_m(\xi)] & \mapsto & \left(\frac{F_0(\xi)}{F_i(\xi)}, \ldots, \widehat{\frac{F_i(\xi)}{F_i(\xi)}}, \ldots, \frac{F_m(\xi)}{F_i(\xi)} \right). \end{array}$$

But all functions $\frac{F_j}{F_i}$ are algebraic by definition, so by part d) the map F is algebraic.

2. (a) Show that the algebraic isomorphisms $\mathbb{C} \to \mathbb{C}$ are exactly given by

$$x \mapsto ax + b \text{ for } a \in \mathbb{C}^*, b \in \mathbb{C}.$$

(b) Show that the algebraic isomorphisms $\mathbb{P}^1 \to \mathbb{P}^1$ are exactly given by

$$\varphi_A : [x, y] \mapsto [ax + by, cx + dy] \text{ for } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2.$$

Solution

(a) The algebraic functions $\mathbb{C} \to \mathbb{C}$ are exactly the polynomials $\mathbb{C}[x]$. So assume that $f, g \in \mathbb{C}[x]$ are such polynomials defining mutually inverse functions $\mathbb{C} \to \mathbb{C}$. Then $f(g(x)) = x$, but note that the polynomial $f \circ g$ has degree $\deg(f)\deg(g) = 1$. Thus $\deg(f) = \deg(g) = 1$, so indeed $f(x) = ax + b$. Clearly, f is injective iff $a \neq 0$. In this case, the inverse g is given by $g(y) = a^{-1}y - a^{-1}b$, so indeed it is also algebraic.

(b) Note first that by Exercise 1, part e), the map φ_A is algebraic, because the two homogeneous polynomials $ax + by$ and $cx + dy$ have a common zero $[x, y]$ iff the vectors (a, b), (c, d) are linearly dependent. Moreover, the inverse of φ_A is given by $\varphi_A^{-1} = \varphi_{A^{-1}}$. This follows from Exercise 5 on Sheet 2, because $\varphi_A \circ \varphi_B = \varphi_{AB}$.
Now let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be an isomorphism. We want to show $\varphi = \varphi_A$ for some $A \in \mathrm{GL}_2$. Let $p = \varphi^{-1}([0, 1])$ and $q = \varphi^{-1}([1, 0])$. By replacing φ with $\varphi \circ \varphi_B$ for a different isomorphism φ_B sending $[0, 1]$ to p and $[1, 0]$ to q, we may assume $p = [0, 1], q = [1, 0]$. Now φ defines an isomorphism $\mathbb{C} \cong U_i \xrightarrow{\varphi} U_i \cong \mathbb{C}$ for $i = 0, 1$. By the previous exercise part, we know that φ must then be given as

$$\varphi|_{U_0} : [1, z] \mapsto [1, \gamma z + \delta],$$
$$\varphi|_{U_1} : [w, 1] \mapsto [\alpha w + \beta, 1],$$

where $\gamma, \alpha \neq 0$. In order for these functions to coincide on $U_0 \cap U_1$, we need

$$\gamma z + \delta = \frac{1}{\alpha \frac{1}{z} + \beta} \text{ for } z \in \mathbb{C}^*.$$

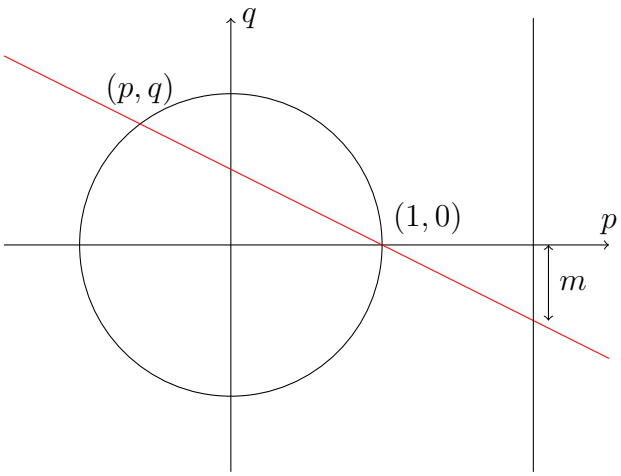
Multiplying with the denominator on the right and expanding, we obtain the equations $\alpha\delta = 0$, $\gamma\beta = 0$ and $\alpha\gamma + \beta\delta = 1$. The first two imply $\delta = \beta = 0$ and thus the third reads $\alpha = \gamma^{-1}$. Then one verifies, that φ agrees with the function φ_A for

$$A = \begin{pmatrix} 1 & 0 \\ 0 & \gamma \end{pmatrix}.$$

3. Find with proof all integer solutions (x, y, z) of the equation $x^2 + y^2 = z^2$.

Solution Apart from the trivial solution $(0, 0, 0)$ we can always assume $z \neq 0$, because squares of real numbers are always nonnegative. Moreover, for (x, y, z) a solution, also (kx, ky, kz) is also a solution. We can thus first determine all

solutions (x, y, z) with x, y, z coprime (which we call *primitive solutions*) and then obtain all solutions simply as multiples of these.
Now for a primitive solution $x^2+y^2 = z^2$, we naturally have $(x/z)^2+(y/z)^2 = 1$ and the rational numbers $p = x/z, q = y/z$ uniquely determine x, y, z up to a sign (as z is the lowest common denominator of p, q). Thus we can equivalently try to classify rational solutions (p, q) of $p^2 + q^2 = 1$.
We know that $(1, 0)$ is certainly a solution and for (p, q) another one, the line through (p, q) and $(1, 0)$ has nonzero, rational slope $m = q/(p-1)$. On the other hand, for $m \in \mathbb{Q} \setminus \{0\}$, the line $q = m(p-1)$ intersects the circle $V(p^2+q^2-1)$ in $(1, 0)$ and one distinct other point.



To compute this point, we insert $q = m(p-1)$ into the above equation and obtain $p^2 + (m(p-1))^2 = 1$. But we already know the solution $p = 1$ so we can draw out a factor $p - 1$

$$p^2 - 1 + m^2(p-1)^2 = (p-1)(p+1+m^2(p-1)) = 0$$

and are left with the equation $p + 1 + m^2(p-1) = 0$ with unique solution $p = (m^2-1)/(m^2+1)$. We insert and obtain $q = m(p-1) = -2m/(m^2+1)$. Again, as m is rational, the point (p, q) is rational. Thus we have seen, that the correspondence from rational solutions $(p, q) \neq (1, 0)$ of $p^2 + q^2 = 1$ to rational numbers m is one-to-one.
To reconstruct the integers x, y, z assume that $m = a/b$ for $b \neq 0$ and a, b coprime. Then we insert and obtain

$$p = \frac{a^2-b^2}{a^2+b^2}, q = \frac{-2ab}{a^2+b^2}.$$

It is tempting to now write $x = a^2 - b^2$, $y = -2ab$, $z = a^2 + b^2$, but we can only conclude this if the three integers $a^2 - b^2$, $a^2 + b^2$ and $2ab$ are coprime. But any prime Q dividing all of them must also divide $(a^2 + b^2) - (a^2 - b^2) = 2b^2$, so $Q = 2$ or $Q|b$. The possibility $Q|b$ can be excluded, as then also $Q|a^2$, a contradiction to a, b coprime.
If $Q = 2$ divides $a^2 - b^2$ then necessarily both a, b are odd (they cannot both be even as they are supposed to be coprime). Then in $q = -2ab/(a^2 + b^2)$ we

can divide denominator and numerator by 2 and we see that the denominator is then odd, so any y in a triple (x, y, z) coming from this q is odd. Now observe that for $x^2 + y^2 = z^2$ with at least one of x, y, z odd, we must have that z and exactly one of x, y is odd. Indeed, odd squares are congruent to 1 modulo 4, so if both x, y were odd, the term $x^2 + y^2$ would be even, but congruent to 2 modulo 4, hence not a square. This would give a contradiction. Hence, by permuting x, y we can assume that x is odd and y is even.
As a result of the above paragraph, all triples (x, y, z) with y even must have $a^2 - b^2$ odd, so exactly one of a, b is odd. In this case, the numbers $a^2 - b^2, a^2 + b^2, 2ab$ are coprime. Thus all primitive triples x, y, z with $x^2 + y^2 = z^2$ are given by

$$x = a^2 - b^2, y = -2ab, z = a^2 + b^2$$

or

$$x = -2ab, y = a^2 - b^2, z = a^2 + b^2$$

with a, b coprime and exactly one of a, b odd. We obtain all possible triples by multiplying the ones above by some $k \in \mathbb{Z}$.

Due March 18.