NOTES (IN PROGRESS)
FOR PROFESSOR SZPIRO'S ALGEBRA II CLASS 2003-04
These are student notes and have not been reviewed by professor Szpiro

1 Algebraic Dynamics

Our aim is to study iterates of maps from the Riemann sphere ($\mathbf{P^1}(\mathbf{C})$) to itself. The iterative process accounts for the "dynamics" in "Algebraic Dynamics". The "algebraicity" stems from the particular maps we will consider: we will take $\varphi(x)$ to be a quotient of two polynomials $P(x)$ and $Q(x)$, with coefficients in a *number field* (a finite extension of $\mathbf{Q}$) or in a *finite field* (that is, $\mathbf{F}_p$, where p is a prime). Henceforward, then, an *algebraic dynamical system* (or *ads*) will be for us an algebraic map:

$$\begin{aligned} \varphi : \mathbf{P^1}(\mathbf{C}) &\rightarrow \mathbf{P^1}(\mathbf{C}) \\ t &\mapsto \frac{P(t)}{Q(t)} \end{aligned}$$

where $P(x)$, $Q(x)$ are polynomials over a number field or finite field.

Moreover, if

$$\varphi(t) = \frac{P(t)}{Q(t)} = \frac{\sum_{i=1}^{n} a_i t^i}{\sum_{j=1}^{m} b_j t^j}$$

we define:

$$\varphi(\infty) = \begin{cases} \infty & if \quad n > m \\ 0 & if \quad n < m \\ a_n/b_m & if \quad n = m \end{cases}$$

$$\begin{aligned} deg\ \varphi(t) &= \sup\ (\deg\ P(t), \deg\ Q(t)) \\ &= \sup(n, m) \\ &= \textit{the number of preimages} \\ &\quad (\textit{not necessarily distinct}) \\ &\quad \textit{of any given image } \varphi(A), \\ &\quad A \in \mathbf{P^1}(\mathbf{C}) \end{aligned}$$

(Indeed, for t $\in \mathbf{P_1}(\mathbf{C})$, the solutions of $\varphi(t) = a$ are exactly those of $P(t) - aQ(t) = 0$. Since deg $(P(t) - aQ(t)) = \sup(n, m)$, there are sup (n, m) solutions (not necessarily distinct) to $P(t) - aQ(t) = 0$, and hence to $\varphi(t) = a$).

We begin our study with a simple

1.1 Example

Let $\varphi : \mathbf{P^1}(\mathbf{C}) \to \mathbf{P^1}(\mathbf{C})$ be given by $\varphi(t) = t^2$. Then the iterates φ^n of φ, $n \in \mathbf{Z}_+$, are given by

$$\varphi^n(t) = \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi(t)}_{n \text{ times}} = t^{2^n}$$

Clearly, the only fixed points of φ (i.e., points t such that $\varphi(t) = t$), are 0, 1, and ∞. As such, these points remain fixed under successive iterates of φ. . . but might there be other fixed points for φ^n, $n > 1$?

Supposing $t \in \mathbf{P^1}(\mathbf{C})$ to be a fixed point of φ^n, we get

$$\begin{aligned} & \varphi^n(t) - t = 0 \\ \Rightarrow \quad & t^{2^n} - t = 0 \\ \Rightarrow \quad & t\,(t^{2^n-1} - 1) = 0 \end{aligned}$$

Thus t may be 0, 1, ∞ or any $(2^n - 1)th$ root of unity. This simple example reflects a general situation for an ads φ: as n increases, so does the number of fixed points for φ^n. The general situation, however, is much more complicated than our example, and hardly allows for the quick identification of fixed points of φ^n. We therefore introduce the useful notion of *preperiodic points*:

Definition 1.1 *The* orbit of a point A under an ads φ, $A \in \mathbf{P^1}(\mathbf{C})$, *is the set* $\{\ \varphi^n(A)$*;* $n \in \mathbf{Z}_+\ \}$

Definition 1.2 *We say that a point* $A \in \mathbf{P^1}(\mathbf{C})$ *is* preperiodic for an ads φ *if the orbit of* A *under* φ *is finite.*

1.2 Example

We saw that the orbit of a point t under $\varphi(t) = t^2$ is given by $\{\ t^{2^n} |\ n \in \mathbf{Z}_+\}$. We claim that $t \neq 0, \infty$ is preperiodic for φ if and only if t is a root of unity.

The orbit of $t = 1$ is clearly finite so suppose that t is a primitive r^{th} root of unity. For any $n \in \mathbf{N}$, there exist $q_n \in \mathbf{N}$, $s_n \in \{0, 1, 2, ..., r-1\}$, such that $2^n = q_n r + s_n$. That is, for any n we have $t^{2^n} = t^{q_n r + s_n} = t^{s_n}$ with $s_n \in \{0, 1, 2, ..., r-1\}$. Thus the orbit of t under φ is contained in the finite set $\{1, t, t^2, ..., t^{r-1}\}$, and t is preperiodic. Conversely, if $t \neq 0, \infty$ is preperiodic, there is an $n \in \mathbf{N}$ such that $t^{2^n} = t^{2^k}$ for some $k \in \{0, 1, 2, ..., n\}$. Then $t^{2^n} - t^{2^k} = 0$, so $t^{2^k}(t^{2^n - 2^k} - 1) = 0$, and t is a root of unity.

Observe that in general, a point A is preperiodic for an ads φ if and only if there exist $n, l \in \mathbf{Z}_+$ such that $\varphi^n(A) = \varphi^{n+l}(A)$. Then $\varphi^n(A) = \varphi^l(\varphi^n(A))$, so that $\varphi^n(A)$ is a fixed point for φ^l. In particular, if the point A itself is a fixed point of some iterate of φ, A is preperiodic. (Note that the converse, however, is false: -1 is preperiodic for $\varphi(t) = t^2$, and yet -1 is not a fixed point of any iterate of φ.)

Finally, we observe that the preperiodic points of an ads φ are algebraic over $\mathbf{Q}$: since φ is a rational function over a number field, so is $\psi_{n,l}(t) = \varphi^{n+l}(t) - \varphi^n(t)$, for any $n, l \in \mathbf{N}$. Thus if a point A in $\mathbf{P^1}(\mathbf{C})$ satisfies $\psi_{n,l}(A) = 0$, we have $A \in \overline{\mathbf{Q}}$.

Definition 1.3 *We say that a point $A \in \mathbf{P^1}(\mathbf{C})$ is a* critical *(or* ramification*)* point for an ads φ *if $\partial\varphi(A) = 0$.*

Note again that if φ is an ads, then so is $\partial\varphi$; so critical points for φ are also algebraic over $\mathbf{Q}$.

Observation 1.4 *Let φ be an ads of degree d. Then A is a critical point for φ if and only if the number of* distinct *preimages for $\varphi(A)$ is strictly less than d.*

Proof: Let $\varphi(t) = P(t)/Q(t)$, $d = \deg \varphi$, $\alpha = \varphi(A)$ $for A$ in $\mathbf{P^1}(\mathbf{C})$. A is a critical point for $\varphi \overset{def}{\Leftrightarrow}$

$$\begin{aligned}
&\partial\varphi(A) = \frac{P'(A)Q(A) - P(A)Q'(A)}{(Q(A))^2} = 0 \\
\Leftrightarrow\ & P'(A)Q(A) = P(A)Q'(A) \\
\Leftrightarrow\ & P'(A)/Q'(A) = P(A)/Q(A) = \varphi(A) = \alpha \\
\Leftrightarrow\ & \begin{cases} P(A) - \alpha Q(A) = 0 \\ P'(A) - \alpha Q'(A) = 0 \end{cases} \\
\Leftrightarrow\ & A \textit{ is a multiple root for } P(t) - \alpha Q(t), \textit{ a polynomial of degree } d
\end{aligned}$$

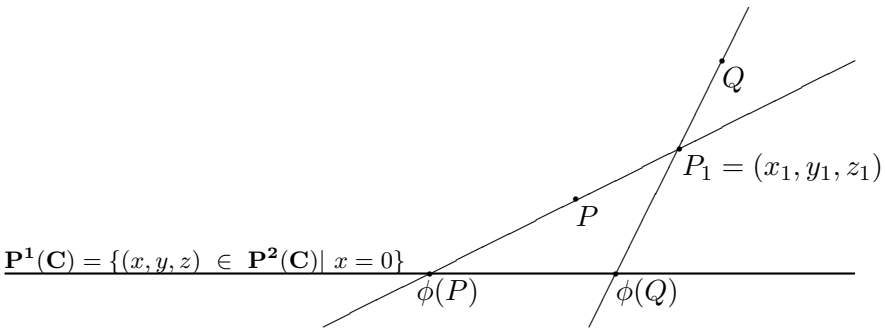
$\Leftrightarrow$ *The number of distinct roots for* $P(t) - \alpha Q(t)$ *is strictly less than* d

$\Leftrightarrow$ *The number of distinct solutions for* $\varphi(t) = \alpha$ *is strictly less than* d

The above observation allows us to speak of the *ramification index* of a ramification point A of φ, by which we mean the multiplicity of A as a preimage of $\varphi(A)$ (or root of $P(t) - \varphi(A)Q(t)$). To develop our intuitive understanding of fixed points and critical points, and to apply some of the notions discussed so far, we turn to a geometric example.

1.3 Example

We first "define" a projection $\phi : \mathbf{P^2}(\mathbf{C}) \to \mathbf{P^1}(\mathbf{C})$ as follows: take a point $P_1 = (x_1, y_1, z_1)$ in $\mathbf{P^2}(\mathbf{C})$. Then for any point $P = (x, y, z)$ in $\mathbf{P^2}(\mathbf{C})$, let $\phi(P)$ be the intersection of the line PP_1 with $\mathbf{P^1}(\mathbf{C})$:

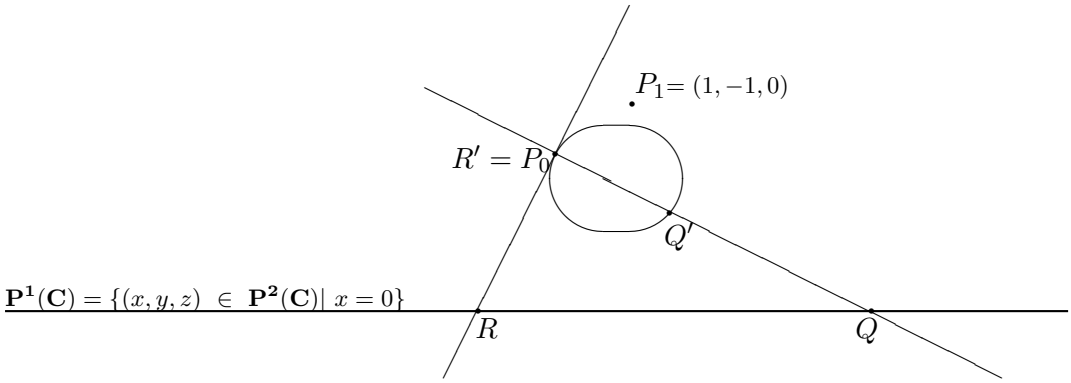


It is clear from our geometric "construction" that ϕ is defined everywhere on $\mathbf{P^2}(\mathbf{C})$ but at $P_1 = (x_1, y_1, z_1)$, and that it depends on P_1. Let us set $P_1 = (1, -1, 0)$. The reader may verify that this yields the map $\phi(P) = \phi(x, y, z) = (x + y, z)$, for $P = (x, y, z) \neq (1, -1, 0)$ in $\mathbf{P^2}(\mathbf{C})$.

We can now use ϕ to construct a map $\varphi : \mathbf{P^1}(\mathbf{C}) \to \mathbf{P^1}(\mathbf{C})$ that involves a projection from a conic $(\mathcal{C})$ in $\mathbf{P^2}(\mathbf{C})$. Recall that a conic is an equation of degree 2 in the plane, that is, any equation of the form:

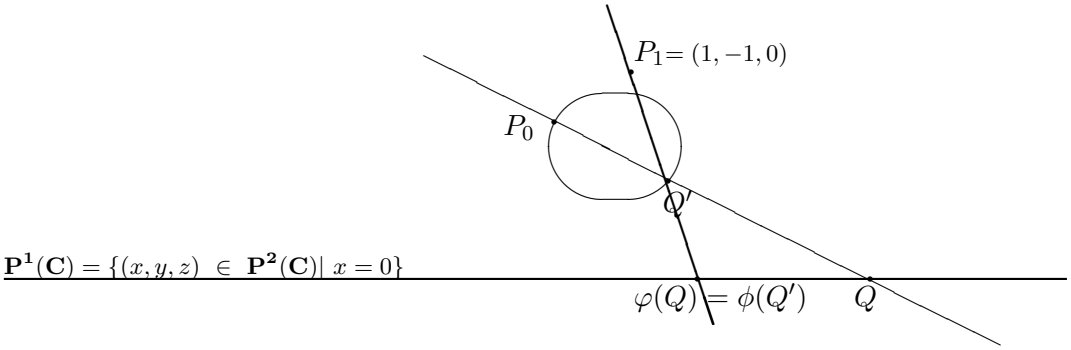
$$A_{00}x^2 + A_{11}y^2 + A_{22}z^2 + A_{01}xy + A_{02}xz + A_{12}yz + A_0x + A_1y + A_2z + A = 0,$$

with (x, y, z) in $\mathbf{P^2}(\mathbf{C})$, and coefficients in $\mathbf{C}$. Let our conic $(\mathcal{C})$ be given by $xy + z^2 = 0$. Then ϕ is defined on $(\mathcal{C})$ since $P_1 \notin (\mathcal{C})$. We now fix a point $P_0 = (x_0, y_0, z_0)$ on $(\mathcal{C})$, and for any point P in $\mathbf{P^1}(\mathbf{C})$, let P' denote the point of intersection of the line PP_0 with $(\mathcal{C})$:



Note that the intersection of a line with a conic *always yields 2 points*: in the picture above, the line QP_0 intersects the conic in two distinct points, while the line RP_0 intersects it in two of the same point. (If a line PP_0 intersects $(\mathcal{C})$ in two distinct points we obviously take P' to be the point of intersection other than P_0.)

Now we "define" φ on $\mathbf{P^1}(\mathbf{C})$ by letting $\varphi(P) = \phi(P')$; that is, $\varphi(P)$ is the intersection with $\mathbf{P^1}(\mathbf{C})$ of the line P_1P':



Naturally, φ depends on where we choose P_0 on the conic. Note that in all cases, φ is defined for every $P \in \mathbf{P^1}(\mathbf{C})$, since ϕ is defined for any $P' \in \mathcal{C}$.

1.4 Exercises

1) Note that the point (1,0,0) satisfies $xy + z^2 = 0$ and hence lies on $\mathcal{C}$. Show that when we set $P_0 = (1, 0, 0)$, we get $\varphi(P) = (P^2 - 1)/P$.

2)Draw a picture to locate the fixed points of φ geometrically. Show that φ has an unique fixed point in $\mathbf{P^1}(\mathbf{C})$, and determine its coordinates when $P_0 = (1, 0, 0)$.

3)Locate the ramification points of φ geometrically.

1.5 Solutions

1) Let $P = (x, y) \in \mathbf{P^1}(\mathbf{C})$. Then since we identified $\mathbf{P^1}(\mathbf{C})$ to the set $(x, y, z) \in \mathbf{P^2}(\mathbf{C})|\ x = 0\}$, we have that $P = (0, x, y)$ as a point in $\mathbf{P^2}(\mathbf{C})$, and the points (X, Y, Z) on the line PP_0 are given by

$$\begin{aligned} X &= 0 + \lambda(0 - 1) &&= -\lambda \\ Y &= x + \lambda(x - 0) &&= x + \lambda x \\ Z &= y + \lambda(y - 0) &&= y + \lambda y \end{aligned}$$

Now since $P' = (X, Y, Z)$ is a point of intersection between this line and our conic, its coordinates satisfy the above equations and also that of $\mathcal{C}$, so

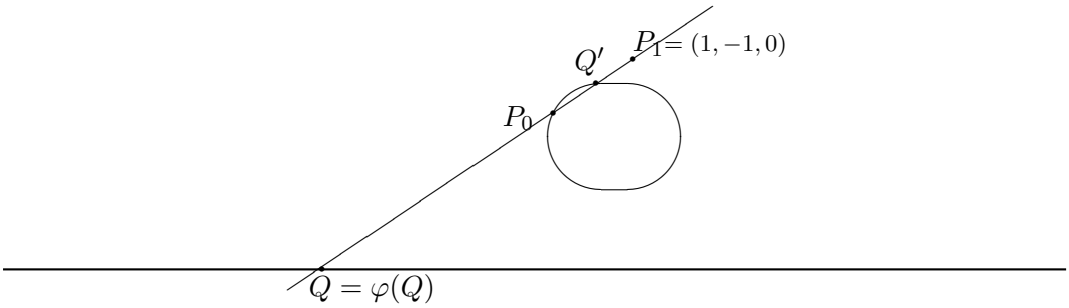
$$\begin{aligned} XY + Z^2 &= 0 && \Rightarrow \\ -\lambda(x + \lambda x) + (y + \lambda y)^2 &= 0 && \Rightarrow \\ -x(\lambda^2 + \lambda) + y^2(\lambda^2 + 2\lambda + 1) &= 0 && \Rightarrow \\ y^2(\lambda + 1) &= -x\lambda && \Rightarrow \\ \frac{\lambda + 1}{\lambda} = 1 + 1/\lambda &= x/y^2 && \Rightarrow \\ 1/\lambda &= (x - y^2)/y^2 && \Rightarrow \\ \lambda &= y^2/(x - y^2) \end{aligned}$$

Substituting λ back into the equation for the line PP_0 yields

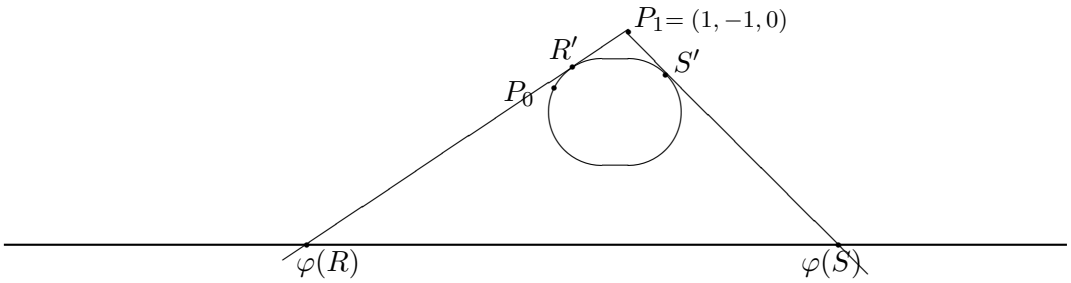
$$\begin{aligned} X &= -y^2/(x - y^2) \\ Y &= x + xy^2/(x - y^2) = x^2/(x - y^2) \\ Z &= y + y^3/(x - y^2) = xy/(x - y^2) \end{aligned}$$

So $P' = (X, Y, Z) = (\frac{-y^2}{x-y^2}, \frac{x^2}{x-y^2}, \frac{xy}{x-y^2}) = (-y^2, x^2, xy)$ and thus $\phi(P') = (x^2 - y^2, xy)$. We have thus shown that for any $P = (x, y) \in \mathbf{P^1}(\mathbf{C})$, $\varphi(x, y) = (x^2 - y^2, xy)$. But $(x^2 - y^2, xy) = (\frac{x^2-y^2}{xy}, 1) = (\frac{x}{y} - \frac{y}{x}, 1) = (\frac{x}{y}, 1) - (\frac{y}{x}, 1) = (x, y) - (y, x) = P - 1/P$, so $\varphi(P) = P - 1/P$.

2) If t is a fixed point of $\varphi(t) = t - 1/t$, then $t = t - 1/t \ \Rightarrow \ t = \infty$. That φ has a unique fixed point is also clear from the picture:



3) Since φ is a map of degree 2, no more than 2 points can yield the same image. Thus in looking for ramification points, we are looking for points whose preimage consists of *only one point*. It is clear from the picture below that $\varphi(R), \varphi(S)$ can each have only one antecedent:



2 Algebraic Dynamics: another example

2.1 Introduction to the Riemann-Harwitz formula

Riemann discovered that an algebraic curve over $\mathbf{C}$ can be identified to a compact Riemann surface with an analytic structure; moreover, the genus g of an algebraic curve corresponds to the number of holes in the associated Riemann surface. We will not prove this, but take it as a fact.

We are already familiar with some compact Riemann surfaces with analytic structures: the Riemann sphere, denoted $\mathbf{P^1}(\mathbf{C})$, is one such; the torus, denoted $\mathbf{C}/\Lambda$, where Λ is a lattice, is another. Since the sphere has no holes, we shall say it is of "genus" 0; similarly we say the torus is of genus 1.

Theorem 2.1 (Riemann-Harwitz formula) *If C_1, C_2 are compact Rie-*

mann surfaces with analytic structures of genuses g_1, g_2 respectively, and

$$\begin{aligned} \varphi: C_1 &\to C_2 \\ t &\mapsto P(t)/Q(t) \end{aligned}$$

is a rational function of degree n, then

$$2g_1 - 2 = n(2g_2 - 2) + \sum_{\textit{critical pts } A \textit{ of } \varphi} (r_A - 1)$$

where r_A denotes the ramification index of a ramification point A of φ.

We will not prove the formula, but use it to obtain information on the ramification points of a given rational map. For example, if φ is defined on the torus $\mathbf{C}/\Lambda$,

$$\begin{aligned} \varphi: \mathbf{C}/\Lambda &\to \mathbf{C}/\Lambda \\ t &\mapsto P(t)/Q(t) \end{aligned}$$

the Riemann-Harwitz formula tells us that $\sum_{\textit{critical pts } A \textit{ of } \varphi}(r_A - 1) = 0$. By definition of r_A, however, we have $r_A \geq 2$ for any critical point A of φ. It follows that φ cannot have any critical points.

To return to the material of section 1, we see that if φ is an ads of degree n, we get $\sum_{\textit{critical pts } A \textit{ of } \varphi}(r_A - 1) = 2n - 2$. In particular, if $\varphi(t) = (t^2 - 1)/t$ as in exercise 1.4, we get

$$\sum_{\textit{critical pts } A \textit{ of } \varphi} (r_A - 1) = 2$$

Now for any critical point A we have $r_A \geq 2$ but also $r_A \leq 2$ since φ is of degree 2. Hence φ has exactly two ramification points, each of index 2. The Riemann-Harwitz formula, in fact, tells us that this is case for any ads of degree 2.

2.2 Defining a group structure on a symmetric curve of degree 3

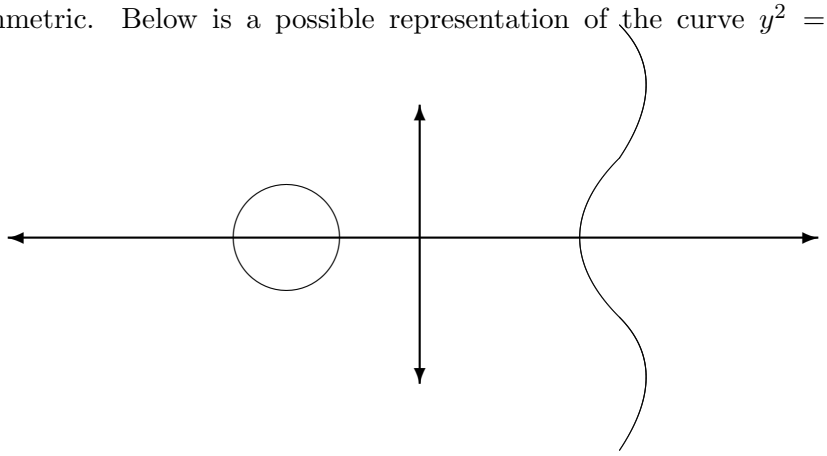
Our aim in this section is to introduce the origins of a particular ads we will subsequently study in some detail. In fact, defining a group structure on a

symmetric curve of degree 3 will lead us naturally to the particular ads

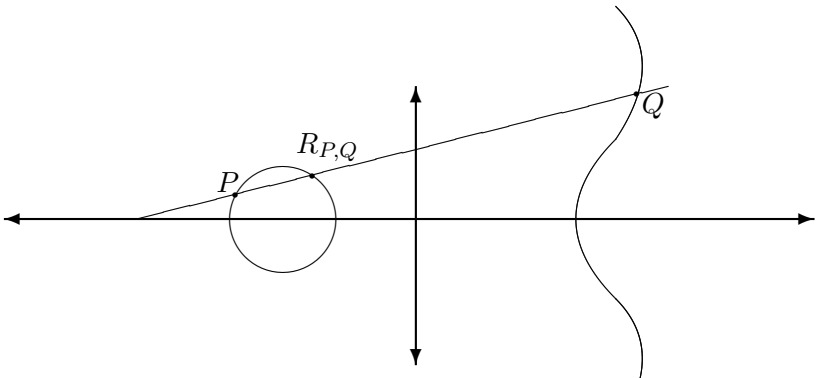
$$\begin{aligned} \varphi : \mathbf{P^1}(\mathbf{C}) &\rightarrow \mathbf{P^1}(\mathbf{C}) \\ x &\mapsto \frac{P'(x)^2 - 8P(x)}{4P(x)} \end{aligned}$$

where P(t) is a polynomial of degree 3.

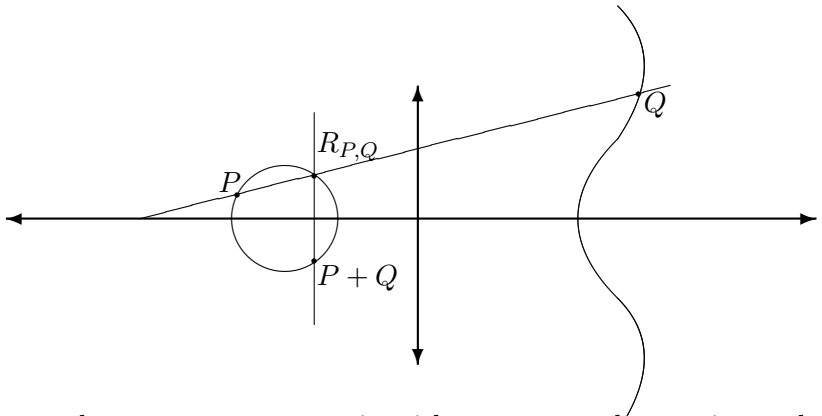
To begin, we let $P(x) = x^3 + px + q$, $y^2 = P(x)$. Note that if y is a solution of $y^2 = P(x)$, then so is $-y$, so the curve so defined is indeed symmetric. Below is a possible representation of the curve $y^2 = P(x)$:



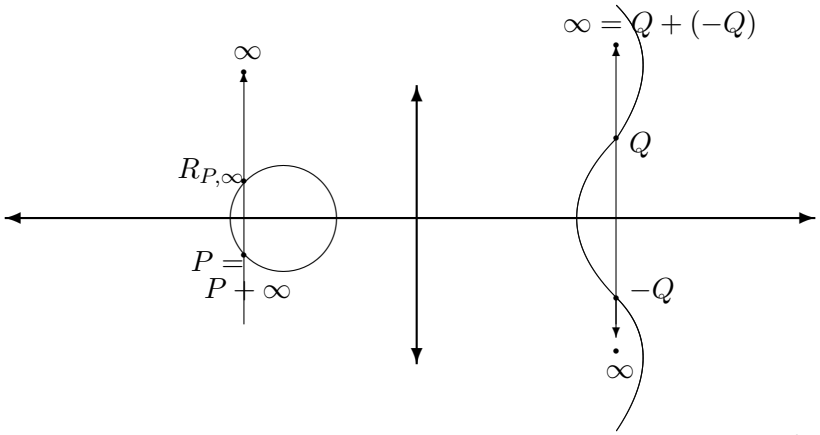
Note that the intersection of a line with a curve of degree 3 always yields three points (not necessarily distinct). Thus, given any two points P, Q on our curve, the line connecting P and Q intersects the curve in a third point $R_{P,Q}$:



Define addition for points on the curve by letting $P + Q$ be *the point symmetric with respect to the x-axis* to this third point of intersection $R_{P,Q}$, as pictured below:



Since we made our curve symmetric with respect to the x-axis, we know that $P + Q$ is a point on the curve; that is, the curve is stable under addition so defined. It is also clear that $+$ is associative, that every point on the curve has an inverse, and that ∞ is the 0-element for $+$:



Thus we have constructed a group $(\mathcal{C},+)$, where $\mathcal{C}$ is the curve $y^2 = x^3 + px + q$.

2.3 Exercises

1) In the group $(\mathcal{C}, +)$ defined above, identify the elements of order 2, and those of order 3.

2) Determine how multiplication by 2 affects the x-coordinate of points on the curve $\mathcal{C}$ (for a point $A = (x, y)$ on the curve, show that the x-coordinate

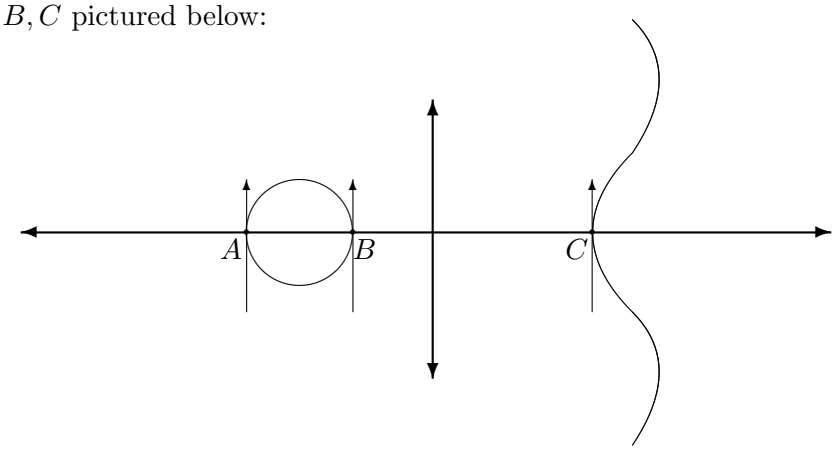
of $2A$ is given by

$$\varphi(x) = \frac{(P')^2 - 8P}{4P} \qquad P = P(x) = x^3 + px + q.)$$

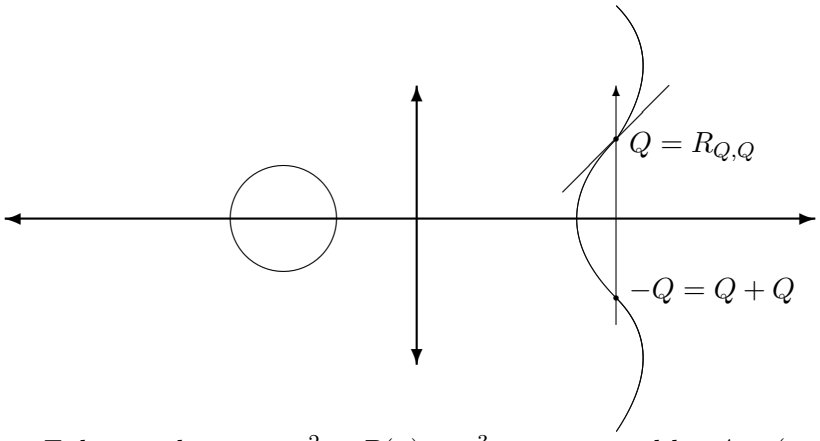
3) Recall that any three points of $\mathbf{P^1}(\mathbf{C})$ can be transformed into any three other points by a transformation of the type $z \mapsto (az + b)/(cz + d)$. So given any three roots of a degree 3 polynomial $P(x)$, we can always think of these roots as 0,1, and some other $a \in \mathbf{P^1}(\mathbf{C})$, and every symmetric curve of degree 3 is then of the form $y^2 = P(x) = x(x-1)(x-a)$. Verify that for any point $A = (x, y)$ on this elliptic curve, the x-coordinate of $2A$ is given by $\varphi(x) = \frac{(x^2-a)^2}{4x(x-1)(x-a)}$.

2.4 Solutions

1) Points P of order 2 in $(\mathcal{C},+)$ verify $2P = 0_{\mathcal{C}} = \infty$ and hence $P = -P$. Since we saw that $-P$ is the point symmetric to P with respect to the x-axis, it follows that the only points besides ∞ of order 2 in $\mathcal{C}$ are the points A, B, C pictured below:



Similarly points Q of order 3 verify $3Q = \infty$ and hence $Q + Q = -Q$. So if Q is of order 3 we must have $R_{Q,Q} = Q$, where $R_{Q,Q}$ is the third point of intersection of the curve with the tangent to the curve at Q. Thus points in $\mathcal{C}$ of order 3 are precisely the inflection points of $\mathcal{C}$ (points Q where the tangent to the curve at Q intersects $\mathcal{C}$ in 3 points instead of 2):



2) Let E denote the curve $y^2 = P(x) = x^3 + px + q$ and let $A = (x, y) \in E$. Then $y^2 = P(x) \Rightarrow 2ydy = P'(x)dx \Rightarrow$ the slope of the line tangent to E at $A = dy/dx = P'(x)/2y$. Thus points (X, Y) on this tangent line are given by

$$X = x + 2y\lambda, \quad Y = y + P'(x)\lambda$$

Since this tangent line at A intersects the cubic E in some third point $R_A = (X, Y)$, substituting in the equation for E yields

$$\begin{aligned}
Y^2 &= P(X) && \Rightarrow \\
(y + P'(x)\lambda)^2 &= P(x + 2y\lambda) && \Rightarrow \\
y^2 + 2y\lambda P'(x) + (P'(x))^2\lambda^2 &\overset{Taylor}{=} P(x) + 2y\lambda P'(x) + 4\lambda^2 y^2 P''(x)/2 \\
&\qquad + 8\lambda^3 y^3 P'''(x)/6 && \Rightarrow \\
(P'(x))^2\lambda^2 &\overset{y^2=P(x)}{=} \lambda^2\,(4y^2 P''(x)/2 + 8y^3\lambda P'''(x)/6) && \Rightarrow \\
(P'(x))^2 &= (4y^2 3x + 8y^3\lambda) && \Rightarrow \\
(P'(x))^2 &= 12P(x)x + 8\lambda y P(x) && \Rightarrow \\
2\lambda y &= \frac{(P'(x))^2 - 12P(x)x}{4P(x)} && \overset{2\lambda y = X - x}{\Rightarrow} \\
X &= \frac{(P'(x))^2 - 8xP(x)}{4P(x)}
\end{aligned}$$

Thus we have calculated the x-coordinate of R_A. But this is also the x-coordinate of $2A$, since $R_A = (X, Y) \Rightarrow A + A = (X, -Y)$, so we are done. Note that multiplication by 2—indeed by n—in $\mathcal{C}$ yields a map from the x-line to the x-line.

3) Easy.

3 Classification of preperiodic points

Definition 3.1 *If A is a fixed point for some iterate φ^n of an ads $\varphi(t)$ (so $\varphi^n(A) = A$) we say that*

A is expanding *if* $|(\varphi^n)'(A)| > 1$
A is contracting *if* $|(\varphi^n)'(A)| < 1$
A is indifferent *if* $|(\varphi^n)'(A)| = 1$

Note that if a critical point A is a fixed point of φ^n, it is necessarily contracting: $\partial\varphi(A) = 0$ since A is a critical point, so $(\varphi^n)'(A) = 0$.

Definition 3.2 *The* Julia set *of an ads φ is the closure of the set of expanding preperiodic points of φ. The* Fatou set *of φ is the complement of the Julia set.*

3.1 Example

We saw that the preperiodic points for the ads $\varphi(t) = t^2$ are $0, \infty$ and the roots of unity. For any root of unity x, we have $|(\varphi^n)'(x)| = |2^n x^{2^n-1}| = 2^n > 1$, so the Julia set in this case is the whole boundary of the unit circle. For the ads $\varphi(t) = \frac{(t^2-a)^2}{4t(t-1)(t-a)}$, it can be shown that the Julia set is precisely $\mathbf{P^1}(\mathbf{C})$.

3.2 Exercises

1)Find the fixed points P of $\varphi(t) = \frac{(t^2-a)^2}{4t(t-1)(t-a)}$. Compute $|\varphi'(P)|$ for these points.

2)Find the preperiodic points of $\varphi(t) = \frac{(t^2-a)^2}{4t(t-1)(t-a)}$.

3.3 Solutions

1)
2)

4 P-adic valuations on $\mathcal{Q}$

To get to the heart of our class, we will need tools to work more deeply with number fields. We begin this section by introducing p-adic valuations on $\mathbf{Q}$,

the associated p-norms on $\mathbf{Q}$, and p-adic fields. We shall then see that we can define on these fields a "height" function, which we will later seek to extend to number fields.

Definition 4.1 *For any prime number p and any $a \in \mathbf{Z}$, the largest power of p which divides a is called* the p-order of a, *denoted $ord_p(a)$. In other words,*

$$ord_p(a) \;=\; \begin{cases} \alpha & if \quad p^\alpha | a,\ p^{\alpha+1} \not| a \\ 0 & if \quad p \not| a \\ \infty & if \quad a = 0 \end{cases}$$

Definition 4.2 *For any prime number p, $a \in \mathbf{Z}$, $b \neq 0 \in \mathbf{Z}$, we define* a p-adic valuation on $\mathbf{Q}$, *denoted v_p, by*

$$\begin{aligned} v_p(a/b) &= ord_p(a) - ord_p(b) \\ v_p(0) &= \infty \end{aligned}$$

Note that $v_p(a) = ord_p(a) \geq 0$ for any $a \in \mathbf{Z}$. Note also that in the definition of v_p we do not require that a and b be coprime, so v_p is well-defined on $\mathbf{Q}$. Indeed if $(a, b) = k \neq 1$, then $a/b = kr/kq$ with $(r, q) = 1$, and

$$\begin{aligned} v_p(a/b) &= ord_p(kr) - ord_p(kq) \\ &= ord_p(r) - ord_p(q) \\ &= v_p(r/q) \end{aligned}$$

4.1 Properties of v_p

For any $x,\ y \in \mathbf{Q}$, we have

$$\begin{aligned} v_p(xy) &= v_p(x) + v_p(y) \qquad (1) \\ v_p(x+y) &\geq \min(v_p(x), v_p(y)) \qquad (2) \end{aligned}$$

The inequality above is generally known as the *ultrametric inequality*. To verify that these properties hold, let $x = a/b,\ y = c/d$, with $b,\ d \neq 0$. Then (1) follows instantly:

$$v_p(xy) \;=\; v_p(ac/bd)$$

$$
\begin{aligned}
&= ord_p(ac) - ord_p(bd) \\
&= ord_p(a) + ord_p(c) - ord_p(b) - ord_p(d) \\
&= v_p(a/b) - v_p(c/d) \\
&= v_p(x) + v_p(y)
\end{aligned}
$$

To verify (2) we may assume without loss of generality that $(a, b) = (c, d) = 1$. We distinguish two cases:

Case 1: Suppose $v_p(a) > 0$ and $v_p(c) > 0$. Then $v_p(b) = v_p(d) = 0$, so $v_p(a/b) = v_p(a)$ and $v_p(c/d) = v_p(c)$. Also, $p^{v_p(a)}$ divides a and $p^{v_p(c)}$ divides c, so $p^{\min(v_p(a),v_p(c))}$ divides both a and c and hence $ab + cd$. It follows that $v_p(ab+cd) \geq \min(v_p(a), v_p(c)) = \min(v_p(a/b), v_p(c/d))$. (The case $v_p(b) > 0,\ v_p(d) > 0$ is treated analagously).

Case 2: Suppose $v_p(a) > 0$ and $v_p(d) > 0$. Then $v_p(a/b) = v_p(a) > 0$ and $v_p(c/d) = -v_p(d) < 0$, so $\min(v_p(a/b), v_p(c/d)) = -v_p(d)$. But now $v_p(a/b + c/d) = v_p(\frac{ad+bc}{bd}) = v_p(ad + bc) - v_p(bd) = v_p(ad + bc) - v_p(d) \geq -v_p(d) = \min(v_p(a/b), v_p(c/d))$, so that $v_p(a/b+c/d) \geq \min(v_p(a/b), v_p(c/d))$ as desired. (The same reasoning again applies to the case $v_p(b) > 0$ and $v_p(c) > 0$).

The v_p valuation now allows us to build an absolute value on $\mathbf{Q}$:

Definition 4.3 *For any prime number p,* the p-adic absolute value on $\mathbf{Q}$, *denoted $\| \ \|_p$, is given by*

$$\| \ x \ \|_p = \ p^{-v_p(x)}, \ \forall x \in \mathbf{Q}$$

Theorem 4.4 *$\| \ \|_p$ is a norm on $\mathbf{Q}$.*

Proof: Clearly $\| \ x \ \|_p \geq 0$ for all $x \in \mathbf{Q}$ and $\| \ x \ \|_p = \ 0 \Leftrightarrow x = 0$. Moreover by the first property of v_p we get $\| \ xy \ \|_p = \| \ x \ \|_p \| \ y \ \|_p$ for all $x, y \in \mathbf{Q}$. Finally we claim $\| \ x + y \ \|_p \leq \| \ x \ \|_p + \| \ y \ \|_p$: the ultrametric inequality tells us that $\| \ x + y \ \|_p = \ p^{-v_p(x+y)} \ \leq \ p^{-\min(v_p(x),v_p(y))}$. Since $p^{-\min(v_p(x),v_p(y))} \ \leq \| \ x \ \|_p + \| \ y \ \|_p$, the claim follows.

We observe in passing that the norms $\|\|_p$ for primes p, together with the usual norm on $\mathbf{Q}$ (which satisfies the triangle inequality but certainly not the stronger ultrametric), in fact account for all norms on $\mathbf{Q}$. That is, any norm on $\mathbf{Q}$ is of one of the two types above. We also refer to these norms

as *places*, usually denoted by v: the usual norm $|\ |$ corresponds to a *place at* ∞, denoted $v = \infty$, and the norms $\|\ \|_p$ are called *finite places* and denoted $v = p$. In what follows, we take advantage of this simpler notation, and will use "all places" to mean "all norms".

Theorem 4.5 (*product formula*) *For any nonzero* $x \in \mathbf{Q}$,

$$\prod_{all\ places\ v} \| x \|_v = 1$$

Proof: It suffices to prove the claim for nonzero $x \in \mathbf{Z}$ since $\| \frac{a}{b} \|_v = \frac{\|a\|_v}{\|b\|_v}$ for any place v and any nonzero $a, b \in \mathbf{Z}$. Let $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where the $p_i,\ i = 1, 2, \dots, k$, are distinct primes. Then

$$\begin{aligned} \| x \|_\infty &= \prod_{i=1}^{k} p_i^{\alpha_i} \\ \| x \|_{p_i} &= p_i^{-\alpha_i}, \quad i = 1, 2, \dots, k \\ \| x \|_p &= 1 \qquad if\ p \neq p_i\ \forall\ i \end{aligned}$$

$$And\ \ thus \qquad \prod_{all\ places\ v} \| x \|_v = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k} p_i^{-\alpha_i} = 1$$

The product formula now allows us to define a "height" function on $\mathbf{P^1}(\mathbf{Q})$:

Definition 4.6 *For any point* $P = (x, y) \in \mathbf{P^1}(\mathbf{Q})$, *the* exponential height of P, *denoted* $H(P)$, *is given by* $H(P) = \prod_{all\ places\ v} \sup(\| x \|_v, \| y \|_v)$

We verify that the function so described is well-defined: for any $(x, y) \in \mathbf{P^1}(\mathbf{Q})$, $\lambda \in \mathbf{Q}$, we have $(x, y) = (\lambda x, \lambda y)$, and so must confirm that $H(\lambda x, \lambda y) = \prod_{all\ places\ v} \sup(\| x \|_v, \| y \|_v)$. Note that $\| \lambda x \|_v = \| \lambda \|_v \| x \|_v$ for any $x,\ \lambda \in \mathbf{Q}$. Then

$$\begin{aligned} \prod_{all\ places\ v} \sup(\| \lambda x \|_v, \| \lambda y \|_v) &= \prod_{all\ places\ v} \sup(\| \lambda \|_v \| x \|_v, \| \lambda \|_v \| y \|_v) \\ &= \prod_{all\ places\ v} \| \lambda \|_v \ \sup(\| x \|_v, \| y \|_v) \end{aligned}$$

$$= (\prod_{all\ places\ v} \| \lambda \|_v)(\prod_{all\ places\ v} \sup(\| x \|_v, \| y \|_v))$$
$$= \prod_{all\ places\ v} \sup(\| x \|_v, \| y \|_v),$$

since $\prod_{all\ places\ v} \| \lambda \|_v = 1$ by the product formula. The height function is thus well-defined, and we have as a corollary:

Corollary 4.7 *Let $(x, y) \in \mathbf{P^1}(\mathbf{Q})$. If $(x, y) = (a, b)$ with $a, b \in \mathbf{Z}$ such that $(a, b) = 1$, then $H(x, y) = \sup(| a |, | b |)$.*

Proof: It suffices to show that $\prod_{all\ \mathbf{finite}\ places\ v} \sup(\| a \|_v, \| b \|_v) = 1$. We note that given any prime p and any $n \in \mathbf{Z}$, $\| n \|_p = p^{-ord_p(n)} \leq 1$, with equality if and only if p does not divide n. Since $(a, b) = 1$, no prime p can divide both a and b, so for any given p we have $\| a \|_p = 1$ or $\| b \|_p = 1$. That is, $\sup(\| a \|_p, \| b \|_p) = 1$ for all p, and our claim follows.

5 (Extending the height function to) Number Fields

Throughout what follows we take $\mathbf{K}$ to be a number field (a finite extension of $\mathbf{Q}$), and $\mathcal{R}$ to be a subring of $\mathbf{K}$.

Definition 5.1 *We say that $x \in \mathbf{K}$ is* integral over $\mathbf{Z}$ *(respectively* over $\mathcal{R}$*) if it satisfies a monic equation with coefficients in $\mathbf{Z}$ (resp $\mathcal{R}$). If $x \in \mathbf{K}$ is integral over $\mathbf{Z}$ we also say that x is an* integral element *of $\mathbf{K}$.*

Example $\sqrt{2}$ is integral over $\mathbf{Z}$ in $\mathbf{K} = \mathbf{Q}(\sqrt{\mathbf{2}})$, since $\sqrt{2}$ satisfies the monic equation $x^2 - 2 = 0$.
Also, $1/2 + \sqrt{5}/2$ is integral over $\mathbf{Z}$ in $\mathbf{K} = \mathbf{Q}(\sqrt{\mathbf{5}})$, since $(1/2 + \sqrt{5}/2) + (1/2 - \sqrt{5}/2) = 1$, $(1/2 + \sqrt{5}/2)(1/2 - \sqrt{5}/2) = -1$ and hence $(1/2 + \sqrt{5}/2)$ satisfies the monic equation $x^2 - x - 1 = 0$.
However, $\sqrt{2/3}$ is not integral over $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{\mathbf{2}}, \sqrt{\mathbf{3}})$.

Definition 5.2 *The set of $x \in \mathbf{K}$ which are integral over $\mathbf{Z}$ (resp $\mathcal{R}$) is called the* integral closure of $\mathbf{Z}$ *(resp $\mathcal{R}$)* in $\mathbf{K}$.
The integral closure of $\mathbf{Z}$ in $\mathbf{K}$ is also called the ring of integers of $\mathbf{K}$, *and is usually denoted Θ_K.*

Theorem 5.3 *The integral closure of $\mathbf{Z}$ (resp $\mathcal{R}$) in $\mathbf{K}$ is a ring.*

In other words, if x and y in $\mathbf{K}$ are integral over $\mathbf{Z}$ (resp $\mathcal{R}$), then so are $x+y$ and xy.

Theorem 5.4 *Let* $\mathbf{K}$ *be a second-degree extension of* $\mathbf{Q}$. *Then this extension is of the form* $\mathbf{K} = \mathbf{Q}(\sqrt{d})$, *where* $d \in \mathbf{Z}$ *is square-free, and*

$$\Theta_K \quad = \quad \begin{cases} \mathbf{Z}[\sqrt{d}] & if \quad d \equiv 2 \text{ or } 3 \ (mod\ 4) \\ \mathbf{Z}[\sqrt{d}/2] & if \quad d \equiv 1 \ (mod\ 4) \end{cases}$$

Example For $\mathbf{K} = \mathbf{Q}(\sqrt{\mathbf{5}})$, we have $\Theta_K = \mathbf{Z}[\sqrt{5}/2]$. It follows immediately that $1/2 + \sqrt{5}/2$ is integral in $\mathbf{Q}(\sqrt{\mathbf{5}})$.

We wish now to establish a product formula for number fields, and to be able to say that for any nonzero x in a number field $\mathbf{K}$ we have $\prod_{all\ places\ v\ of\ K} \| x \|_v = 1$. But for this we need to understand what the 'places' of a number field $\mathbf{K}$ correspond to. Again, we distinguish two categories. Places at infinity correspond to *archimedean absolute values* $|\ |$, which satisfy the following for all x, y in $\mathbf{K}$:

$$\begin{array}{rrcl} (i) & | x | & \geq & 0 \\ (ii) & | xy | & = & | x || y | \\ (iii) & | x + y | \leq & | x | + | y | \end{array}$$

Finite places correspond to *non-archimedean absolute values* $|\ |$, which satisfy not only (i) and (ii) above but also the ultrametric inequality $| x+y | \leq \max(| x |, | y |)$, stronger than inequality (iii). We examine now in more detail the distinction between archimedean and non-archimedean places.

5.1 Archimedean Places

Recall that if $\mathbf{K}$ is a number field, it is embeddable in the complex field $\mathbf{C}$ by a field homomorphism $\sigma : \mathbf{K} \hookrightarrow \mathbf{C}$ that fixes $\mathbf{Q}$ and sends $\alpha \in \mathbf{K}$ to roots of the minimal polynomial for α over $\mathbf{K}$. Many different such embeddings are possible: for example in the case $\mathbf{K} = \mathbf{Q}(\sqrt{2})$, we have the possible embeddings:

$$\begin{array}{lll} \sigma_1 : \mathbf{K} \hookrightarrow \mathbf{R} & & \sigma_2 : \mathbf{K} \hookrightarrow \mathbf{R} \\ \sqrt{2} \mapsto \sqrt{2} & & \sqrt{2} \mapsto -\sqrt{2} \end{array}$$

Theorem 5.5 *If* $\mathbf{K}$ *is a number field, the number of distinct embeddings* $\sigma : \mathbf{K} \hookrightarrow \mathbf{C}$ *is equal to* $[K : Q]$*, the degree of* $\mathbf{K}$ *over* $\mathbf{Q}$*.*

Archimedean absolute values on $\mathbf{K}$ are determined by these embeddings: the norm $|\ |_\sigma$ corresponding to an embedding σ is given by $|\ x\ |_\sigma = |\ \sigma(x)\ |$ (where $|\ |$ is the usual norm on $\mathbf{C}$). In saying this, however, we must be careful, for distinct embeddings do not necessarily yield different norms. In fact this is only the case if σ is a real embedding ($\sigma(K) \subset \mathbf{R}$). If σ is complex, then the embedding $\overline{\sigma}$ given by $\overline{\sigma}(x) = \overline{\sigma(x)}\ \forall x \in \mathbf{K}$ is clearly a distinct embedding, but the the two yield the same norm since $|\ \sigma(x)\ | = |\ \overline{\sigma}(x)\ |$.