12 Liouville's theorem. Fundamental theorem of algebra

One of the immediate consequences of Cauchy's integral formula is Liouville's theorem, which states that an entire (that is, holomorphic in the whole complex plane $\mathbf{C}$) function cannot be bounded if it is not constant. This profound result leads to arguably the most natural proof of *Fundamental theorem of algebra*. Here are the details.

12.1 Liouville's theorem

Theorem 12.1. *Let f be entire and bounded. Then f is constant.*

Proof. Take two arbitrary points $a, b \in \mathbf{C}$ and let γ_R be the circle $\partial B(0, R)$, where R is chosen so big that $|z - a| \geq R/2$ and $|z - b| \geq R/2$ for all points $z \in \gamma_R$. For both points Cauchy's integral formula holds:

$$f(a) = \frac{1}{2\pi \mathrm{i}} \int_{\gamma_R} \frac{f(z)}{z - a} \mathrm{d}z, \quad f(b) = \frac{1}{2\pi \mathrm{i}} \int_{\gamma_R} \frac{f(z)}{z - b} \mathrm{d}z.$$

Therefore,

$$|f(a) - f(b)| = \frac{|a - b|}{2\pi} \left| \int_{\gamma_R} \frac{f(z)}{(z - a)(z - b)} \mathrm{d}z \right|.$$

By the assumption $|f(z)| \leq M$ for some constant M and hence on γ_R

$$\left| \frac{f(z)}{(z - a)(z - b)} \right| \leq \frac{4M}{R^2}.$$

This implies, by the ML–inequality,

$$|f(a) - f(b)| \leq \frac{4M}{R^2} \frac{|a - b|}{2\pi} \operatorname{length} \gamma_R = |a - b| \frac{4M}{R} \to 0, \quad R \to \infty.$$

Therefore $f(a) = f(b)$, and since a, b were arbitrary, f must be constant. ∎

12.2 Fundamental theorem of algebra

Recall that a polynomial $p\colon \mathbf{C} \to \mathbf{C}$ is a function of the form

$$p(z) = c_n z^n + c_{n-1} z^{n-1} + \ldots + c_1 z + c_0,$$

where $c_0, \ldots, c_n$ are some given complex constant. I assume that $c_n \neq 0$. If $n \geq 1$ then the polynomial is non-constant. Any polynomial is an entire function, and therefore continuous. Complex number $\hat{z}$ is called a root of polynomial p if $p(\hat{z}) = 0$. Now I am ready to state and, more importantly, prove the following theorem.

Theorem 12.2. *Every non-constant polynomial p has at least one root $\hat{z} \in \mathbf{C}$.*

Math 452: *Complex Analysis* by Artem Novozhilov©
e-mail: artem.novozhilov@ndsu.edu. Spring 2019

Proof. I will prove this theorem by contradiction assuming that there is a nonconstant polynomial p with no root. First I note that for any non-constant polynomial $p(z) \to \infty$ as $z \to \infty$ (recall that complex plane has only one infinity). Indeed,

$$p(z) = z^n \left(c_n + \frac{c_{n-1}}{z} + \ldots + \frac{c_0}{z^n} \right),$$

and since $z^n \to \infty$ as $z \to \infty$ I obtain the required conclusion. Now take sufficiently large ball $B(0, R)$. By the proven $|p(z)| > M$ outside this ball for some constant M, and I can always choose R big enough to guarantee that

$$\frac{1}{|p(z)|} < 1,$$

for all $z \notin B(0, R)$. Since I assumed that p has no roots, function

$$z \mapsto \frac{1}{p(z)}$$

is entire, and in particular it is holomorphic inside $B(0, R)$, and hence continuous on $\overline{B}(0, R)$. Continuous functions on compact sets attain their maximum and minimum values and in particular bounded, hence

$$\frac{1}{|p(z)|} \leq B,$$

for some constant B and $z \in \overline{B}(0, R)$. This implies that the entire function $1/p$ is bounded in $\mathbf{C}$ and hence, by Liouville's theorem, constant, which contradicts the assumption that p is non-constant. ■

Remark 12.3. In a more algebraic fashion the previous theorem sometimes is stated as "The filed of complex numbers $\mathbf{C}$ is algebraically closed."

Here is an important consequence of this theorem, which sometimes also called the fundamental theorem of algebra.

Theorem 12.4. *Any complex polynomial $p\colon \mathbf{C} \to \mathbf{C}$ can be uniquely factored (up to the permutation of the factors) as*

$$p(z) = c_n (z - \hat{z}_1)^{\alpha_1} (z - \hat{z}_2)^{\alpha_2} \ldots (z - \hat{z}_k)^{\alpha_k},$$

where $\hat{z}_1, \ldots, \hat{z}_k$ are the roots of p, and $\alpha_1, \ldots, \alpha_k$ are the corresponding multiplicities, that satisfy $\alpha_1 + \ldots + \alpha_n = n$.

In other words, every complex polynomial of degree n has exactly n complex roots counting each root according to its multiplicity.

Proof. Let p be a polynomial of degree n. If $n = 0$ we are done. If $n \geq 1$ by the fundamental theorem of algebra there must be $\hat{z} \in C$ such that

$$p(\hat{z}) = 0.$$

I claim that this is equivalent to the fact that polynomial p can be written as the product of $(z - \hat{z})$ and another polynomial q of degree $n - 1$:

$$p(z) = (z - \hat{z}) q(z).$$

Indeed, one direction is obvious (let $\hat{z}$ be such that $p(\hat{z}) = 0$ then $(z-\hat{z})q(z) = 0$ as well). In the other direction, I will show even more. Specifically, no matter what the number $\hat{z} \in \mathbf{C}$ is (non necessarily a root), there exist complex constant $a_1, \ldots, a_n$ such that polynomial can be written as

$$p(z) = a_0 + a_1(z - \hat{z}) + \ldots + a_n(z - \hat{z})^n.$$

The proof is direct, by construction. Take $w = z - \hat{z}$, therefore $z = w + \hat{z}$, and $p(z) = p(w + \hat{z}) = \tilde{p}(w) = c_0 + \ldots + c_n(w + \hat{z})^n$. Raise all the terms to the corresponding power, simplify, and end up with $\tilde{p}(w) = a_0 + a_1 w + \ldots + a_n w^n$, hence $p(z) = \tilde{p}(z - \hat{z})$ has the required form. Note that $c_n = a_n$ and $a_0 = p(\hat{z})$.

Now I can rearrange my polynomial as follows

$$p(z) = a_0 + (z - \hat{z})(a_1 + a_2(z - \hat{z}) + \ldots + a_n(z - \hat{z})^{n-1}) = a_0 + (z - \hat{z})q(z),$$

where q has degree $n - 1$. From the last expression I obtain the required conclusion that if $p(z) = (z - \hat{z})q(z)$ then $\hat{z}$ must be a root (since $a_0 = 0 = p(\hat{z})$).

We are basically done, since, due to fact that q is a complex polynomial of degree $n-1$, it is either constant ($n = 1$) or, by fundamental theorem of algebra, has a complex root $\hat{w}$, therefore,

$$q(z) = (z - \hat{w})h(z),$$

where h has degree $n - 2$, and so on.

I will leave to prove the uniqueness of such factorization to the reader. ■

Remark 12.5. In complex analysis very often the term "root" is replaced with the term "zero." And in general *zeros of functions* and their corresponding multiplicities are studied. In the following I will stick to this terminology.

Example 12.6. Consider

$$p(z) = z^4 + (2 + \mathrm{i})z^3 - (2 - 5\mathrm{i})z^2 - (4 + 5\mathrm{i})z + (3 - \mathrm{i}),$$

which is a polynomial of degree 4. Therefore there must be 4 (counting multiplicities) complex roots. Indeed, one can check that i is a root of multiplicity 2 and $1, -3 + \mathrm{i}$ are the roots multiplicity 1, that is,

$$p(z) = (z + \mathrm{i})^2(z - 1)(z + 3 - \mathrm{i}).$$