ANALYTIC AND COMBINATORIAL NUMBER THEORY
(NDMI045)
summer term 2020/21
lecturer: Martin Klazar

LECTURE 1 (4.3.2021). TWO EXAMPLES. THE FUNDAMENTAL THEOREM OF ALGEBRA.

• ANALYTIC ... continuous and analytic functions, derivatives, integrals, methods of mathematical analysis
• COMBINATORIAL ... applications to combinatorial problems, to $\mathbb{Z}$ (the integers) and other discrete objects
• implicit is ALGEBRAIC ... applications of formal power series

Let us give a few examples. $\underline{\mathbb{N} = \{1, 2, \dots\}}$ are the natural numbers and $\underline{\mathbb{N}_0 = \{0, 1, 2, \dots\}}$ $(= \mathbb{N} \cup \{0\})$ are the nonnegative integers.

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

are the integers. For $a, d \in \mathbb{N}$,

$$a + d\mathbb{N}_0 := \{a + dn \mid n \in \mathbb{N}_0\} = \{a, a + d, a + 2d, \dots\}$$

is an (infinite) <u>arithmetic progression</u>, shortly <u>AP</u>, where d is called the <u>common difference</u>. Here are some partitions of $\mathbb{N}$ in APs:

$$\begin{aligned} \mathbb{N} &= (1 + 2\mathbb{N}_0) \cup (2 + 2\mathbb{N}_0) = \{1, 3, 5, \dots\} \cup \{2, 4, 6, \dots\} \\ &= (1 + 4\mathbb{N}_0) \cup (3 + 4\mathbb{N}_0) \cup (2 + 2\mathbb{N}_0) \\ &= (1 + 8\mathbb{N}_0) \cup (5 + 8\mathbb{N}_0) \cup (3 + 4\mathbb{N}_0) \cup (2 + 2\mathbb{N}_0) \\ &\vdots \end{aligned}$$

— note that always some common difference is repeated.

Theorem 1. *No partition*

$$\mathbb{N} = \bigcup_{i=1}^{k} (a_i + d_i\mathbb{N}_0)$$

exists such that $k \in \mathbb{N}$, $a_i, d_i \in \mathbb{N}$, and $1 \le d_1 \le d_2 \le \cdots \le d_{k-1} < d_k$ — the largest common difference has to be repeated.

Proof. *Analytic proof.* Any partition $\mathbb{N} = \bigcup_{i=1}^{k}(a_i + d_i\mathbb{N}_0)$ is equivalent with the equality of functions ($z \in \mathbb{C}$)

$$\sum_{n\in\mathbb{N}} z^n = \frac{z}{1-z} = \sum_{i=1}^{k} \frac{z^{a_i}}{1-z^{d_i}} = \sum_{i=1}^{k} \sum_{n\in a_i+d_i\mathbb{N}_0} z^n,\ |z|<1$$

— recall that $\sum_{n=0}^{\infty} z^{a+dn} = z^a/(1-z^d)$. We assume, for contradiction, that $1 \le d_1 \le d_2 \le \cdots \le d_{k-1} < d_k$. We take a sequence $(z_n) \subset \mathbb{C}$ such that $|z_n| < 1$ and

$$z_n \to \alpha := e^{2\pi i/d_k}\ ,$$

and set $z := z_n$. The LS $\to \frac{\alpha}{1-\alpha}$ but the RS $\to \sum_{i=1}^{k-1} \alpha^{a_i}/(1-\alpha^{d_i}) + \infty = \infty$, which is a contradiction.

Algebraic proof. We actually do not need to substitute anything for z and can keep it a formal variable, because the equality

$$\frac{z}{1-z} = \sum_{i=1}^{k} \frac{z^{a_i}}{1-z^{d_i}} \qquad (*)$$

with $d_k > 1, d_1, \ldots, d_{k-1}$ is impossible already from a purely algebraic reason. It is the same reason by which we know that, for example,

$$\frac{23}{100} - \frac{25}{72} + \frac{22}{26} - \frac{33}{35} \neq 0\ ,$$

even without evaluating the expression. The reason is that these fractions are in lowest terms and the prime number $p = 13$ occurs exactly once as a divisor of the denominator, namely in the third fraction. Thus we bring the expression on a common denominator as

$$\frac{a+13b}{13c},\ a,\ b,\ c \in \mathbb{Z},\ c \neq 0\ ,$$

and with a not divisible by 13. Thus $a + 13b \neq 0$ and the expression is nonzero. This uses unique prime factorization in the ring $\mathbb{Z}$. In equation $(*)$ we use unique prime factorization in the ring $\mathbb{C}[z]$ and the irreducible element $p = z - \alpha$ in it that divides the denominator $z^{d_k} - 1$ but not the others. □

A nice slim (76 pp.) book about applications of analytic methods in number theory is D. J. Newman's *Analytic Number Theory*, Springer-Verlag, 1998. The previous example (but not the algebraic proof!)

is taken from it, and it contains many more similar gems. *Donald J. Newman (1930, Brooklyn, NY – 2007, Philadelphia, Pennsylvania)* is most famous for his short proof (in 1980) of the Prime Number Theorem, which says that

$$\pi(x) = \#\{p \mid p \le x \wedge p \text{ is a prime number}\} \sim \frac{x}{\log x} \quad \text{as} \quad x \to +\infty \,.$$

Surely enough, he presents it in his book. I hope to present it in my lectures too.

An integer partition (above we considered set partitions), shortly a partition, of $n \in \mathbb{N}$ is an expression $n = a_1 + a_2 + \cdots + a_k$ where $a_i \in \mathbb{N}$ and the order of summands does not matter. More formally, it is a k-tuple

$$\lambda = (a_1, a_2, \ldots, a_k) \in \mathbb{N}^k \quad \text{such that} \quad a_1 \ge a_2 \ge \cdots \ge a_k \ge 1 \quad \text{and} \quad \sum_{i=1}^{k} a_i = n \,.$$

We write $\lambda \vdash n$ and say that the a_i are parts of λ. Another format for λ is

$$\lambda = n^{m_n}\,(n-1)^{m_{n-1}}\,\ldots\,1^{m_1} \quad \text{where } m_i \in \mathbb{N}_0 \text{ and } \sum_{i=1}^{n} m_i \cdot i = n \,.$$

The m_i are multiplicities of the parts i. Exponents 1 are omitted, as well as powers with exponent 0. For illustration we list all seven partitions of 5 in both formats:

$$(5),\ (4,\,1),\ (3,\,2),\ (3,\,1,\,1),\ (2,\,2,\,1),\ (2,\,1,\,1,\,1),\ (1,\,1,\ 1,\,1,\,1)$$

and

$$5,\ 41,\ 32,\ 31^2,\ 2^2 1,\ 21^3,\ 1^5 \,.$$

Besides the PNT another famous result in analytic (and combinatorial) number theory is the asymptotic formula for the partition function $p(n) = \#\{\lambda \mid \lambda \vdash n\}$ which counts partitions of n, namely

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}} \quad \text{as} \quad n \to \infty \,.$$

It was found by *Godfrey H. Hardy (1877–1947)* and *Srinivasa Ramanujan (1887–1920)* in 1918, and slightly later independently by *James V. Uspensky (1883–1947)*. D. J. Newman gave a relatively

short analytic proof of it in *Michigan J. Math.* in 1962. I think that this time I will also present a proof of it in my lectures.

If we underline in the list of partitions of 5 those with distinct parts (i.e. $m_i \leq 1$) and overline those with only odd parts —

$$\underline{\overline{5}},\ \underline{41},\ \underline{32},\ \overline{31^2},\ 2^21,\ 21^3,\ \overline{1^5}$$

— we see that we have three partitions of each kind. This holds in general.

Theorem 2 (L. Euler) *For every $n \in \mathbb{N}$ we have that $p_d(n) = p_o(n)$, where*

$$p_d(n) := \#\{\lambda \vdash n \mid \lambda \textit{ has distinct parts}\} \quad \textit{and}$$
$$p_o(n) := \#\{\lambda \vdash n \mid \lambda \textit{ has odd parts}\}\ .$$

Proof. *Analytic proof.* For every $z \in \mathbb{C}$ with $|z| < 1$ we have that

$$F_d(z) := \sum_{n=0}^{\infty} p_d(n) z^n = \prod_{n=1}^{\infty} (1 + z^n)$$

and

$$F_o(z) := \sum_{n=0}^{\infty} p_o(n) z^n = \prod_{n=1}^{\infty} \frac{1}{1 - z^{2n-1}}$$

(as we know, $\sum_{n \geq 0} z^{nd} = 1/(1 - z^d)$). Also, $1 + z^n = \frac{1-z^{2n}}{1-z^n}$. Thus

$$\begin{aligned} F_d(z) &= \prod_{n=1}^{\infty} (1 + z^n) = \prod_{n=1}^{\infty} \frac{1 - z^{2n}}{1 - z^n} = \frac{\prod_{n=1}^{\infty} (1 - z^{2n})}{\prod_{n=1}^{\infty} (1 - z^n)} \\ &= \frac{1}{\prod_{n=1}^{\infty} (1 - z^{2n-1})} = \prod_{n=1}^{\infty} \frac{1}{1 - z^{2n-1}} \\ &= F_o(z)\ , \end{aligned}$$

whence $p_d(n) = p_o(n)$ for every n.

Algebraic proof. The previous short proof hides some analytic considerations, and is complete only when these are made explicit (or at least when one realizes that nontrivial things still remain to be proven). We (i) need to prove that the generating functions $F_d(z)$ and $F_o(z)$ are for $|z| < 1$ really equal to the stated infinite products, (ii) have to justify manipulations with infinite products in the above

computation, and (iii) rely in the above "whence" on an identity theorem for power series (functional equality is equivalent with equality of coefficients). But we may again, as in the previous example, forget about $F_d(z)$ and $F_o(z)$ as functions and regard them as formal power series from the ring $\mathbb{C}[[z]]$. Then (i) is very simple, as it follows from the definitions of the counting quantities $p_d(n)$ and $p_o(n)$, (iii) is inbuilt in the definition of $\mathbb{C}[[z]]$, and only (ii) remains to be shown (one has to justify manipulation with formal infinite products). This algebraic proof is simpler than the original analytic one. $\square$

Let us establish the basic and fundamental property of the field $\mathbb{C}$ of complex numbers, its algebraic closedness; we achieve it by means of the topological notion of connectedness. It is expressed in the *Fundamental Theorem of Algebra*.

Theorem 3 (FTA). *Every non-constant complex polynomial has a root in* $\mathbb{C}$*,*

$$n \in \mathbb{N} \wedge (a_0,\, a_1, \ldots,\, a_n \in \mathbb{C}) \wedge a_n \neq 0$$
$$\Rightarrow \exists\, \alpha \in \mathbb{C} :\ \textstyle\sum_{j=0}^{n} a_j \alpha^j = 0\ .$$

We prove it in two steps.

Step 1 (reduction). *If every polynomial* $z^n + a$*, where* $n \in \mathbb{N}$ *and* $a \in \mathbb{C}$*, has a root in* $\mathbb{C}$*, then the FTA holds.*

and

Step 2 ($\mathbb{C}$ has k-th roots). *The field* $\mathbb{C}$ *is closed to taking any root,*

$$\forall\, k \in \mathbb{N}\ \forall\, a \in \mathbb{C}\ \exists\, b \in \mathbb{C} :\ b^k = a\ .$$

Clearly, Step 1 + Step 2 $\Rightarrow$ FTA.

Proof of Step 1. Let $p(z) = a_0 + a_1 z + \cdots + a_n z^n$ be a degree $n \geq 1$ complex polynomial, so $a_n \neq 0$. It is easy to see that the function

$$\mathbb{C} \ni z \mapsto f(z) := |p(z)| \in [0,\, +\infty)$$

attains at some $z = \alpha \in \mathbb{C}$ its minimum value. It follows from the continuity of $f(z)$ (thus it attains minimum on every compact subset

of $\mathbb{C}$) and the fact, left as an exercise for you, that

$$\lim_{|z|\to+\infty} f(z) = +\infty \ .$$

Using the substitution $z := z - \alpha$, we may assume that the minimum of $f(z)$ is attained at $z = \alpha = 0$ (another exercise for you).

We show that if $f(0) > 0$ then $f(z) < f(0)$ for some point $z \in \mathbb{C}$ (close to 0), which would be a contradiction with the minimality of $f(0)$. So $f(0) = |p(0)| = 0$, $p(0) = 0$ and 0 is a root of $p(z)$. We assume that $a_0 \neq 0$, else we are done immediately. We split $p(z)$ as

$$p(z) = a_0 + a_k z^k + \underbrace{a_{k+1}z^{k+1} + \cdots + a_n z^n}_{q(z)}$$

so that $k \in \mathbb{N}$, $a_0 \neq 0$ and $a_k \neq 0$. Clearly,

$$q(z) = o(z^k) \ \text{ as } \ z \to 0 \ . \tag{o}$$

Using the assumption we take an $\alpha \in \mathbb{C}$ such that

$$\alpha^k = -\frac{a_0}{a_k} \ .$$

By (o) we take a $\delta \in (0,1)$ such that $|q(\delta\alpha)| \leq \frac{1}{2}\delta^k |a_0|$. Then indeed

$$\begin{aligned} f(\delta\alpha) &= |p(\delta\alpha)| = |a_0 - a_0\delta^k + q(\delta\alpha)| \\ &\leq |a_0|(1-\delta^k) + |q(\delta\alpha)| \\ &\leq |a_0|(1-\delta^k/2) \\ &< |a_0| = |p(0)| = f(0) \ . \end{aligned}$$

□

Proof of Step 2. We need to show that for every $k \in \mathbb{N}$ and every $a \in \mathbb{C}$ there is a $\sqrt[k]{a} \in \mathbb{C}$. For $k = 1$ this is trivial and for $k = 2$ it is left as an exercise for you. Also, from real analysis we know that if $a \in [0, +\infty)$ then $\sqrt[k]{a} \in [0, +\infty)$ exists. Thus we may assume that $k \in \mathbb{N}$ is odd and $|a| = 1$ (any $k \in \mathbb{N}$ has form $k = 2^l k'$ with $l \in \mathbb{N}_0$ and odd $k' \in \mathbb{N}$, and for $a \neq 0$ we can replace a with $a/|a|$). We consider the map

$$f(z) = z^k \colon S := \{z \in \mathbb{C} \mid |z| = 1\} \to S$$

and show that it is onto. Recall that a set $X \subset \mathbb{C}$ is disconnected if there exist disjoint open sets $A, B \subset \mathbb{C}$ such that we have a (set) partition

$$X = (X \cap A) \cup (X \cap B)$$

in which both sets in the union are nonempty. Else the set X is connected. It is a well known fact in analysis (and an exercise for you) that if X is connected and $g\colon X \to \mathbb{C}$ is a continuous map then its image $g[X] = \{g(z) \mid z \in X\}$ is connected.

Now suppose for contradiction that $f[S] \neq S$ and take a $c \in S \setminus f[S]$. Since k is odd, $f(-z) = -f(z)$ and $z \in f[S] \Rightarrow -z \in f[S]$, in particular also $-c \in S \setminus f[S]$. We take the line $\ell \subset \mathbb{C}$ going through the points c and $-c$ and define $A, B \subset \mathbb{C}$ to be the open halfplanes determined by the line ℓ. Then the partition

$$f[S] = (f[S] \cap A) \cup (f[S] \cap B)$$

shows that the set $f[S]$ is disconnected. But this is a contradiction with the above fact because S is connected (exercise ...) and f is continuous. □

THANK YOU!