(September 13, 2020)

01. Complex numbers

Paul Garrett  garrett@math.umn.edu  http://www.math.umn.edu/~garrett/

[This document is http://www.math.umn.edu/~garrett/m/complex/notes_2020-21/01_intro.pdf]

1. Constructions/existence of \( \mathbb{C} \)
2. Addition, multiplication, conjugates, norms, metric
3. Convergence of sequences and series, topology

1. Constructions/existence of complex numbers

The various constructions of the complex numbers in terms of other, pre-existing objects are not used ever again, since really these are just existence arguments, adding little to our appreciation of the properties of complex numbers.

Both constructions here are anachronistic, since they use ideas that came decades later than the basic work in complex analysis. Both constructions depend on existence of the real numbers \( \mathbb{R} \), demonstrated only as late as 1871 by Cantor (in terms of Cauchy sequences) and 1872 by Dedekind (in terms of cuts). One construction uses the notion of quotient ring of a polynomial ring, which was not available in the early 19th century.\[1\] The other uses matrix rings, likewise unavailable in the early 19th century.

The first of these two constructions of \( \mathbb{C} \) uses a Kronecker-style construction of an extension field of a given field \( k \), as a quotient of the polynomial ring \( k[X] \) by an ideal generated by an irreducible polynomial. This construction is significant already for making fields such as \( \mathbb{Q}(\sqrt{2}) \) without presuming the existence of \( \sqrt{2} \) in some larger universe, that is, presuming the lack of self-contradiction in existence of \( \sqrt{2} \). Indeed, the usual proof that there is no rational \( \sqrt{2} \) might be interpreted as a proof of its non-existence. The late-19th-century idea is to form \( \mathbb{Q}(\sqrt{2}) \) as a quotient of a polynomial ring

\[
\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[X]/\langle X^2 - 2 \rangle
\]

observing that the image of \( X \) in the quotient is a square root of 2.

The risks of such a presumption loom larger for \( \sqrt{-1} \), since, unlike \( \sqrt{2} \), it is not a limit of rational numbers (with the usual metric). So, granting a sufficient idea of the real numbers \( \mathbb{R} \), a Kronecker-style algebraic construction of the complex numbers as quotient of a polynomial ring in one variable is

\[
\mathbb{C} = \mathbb{R}[X]/\langle X^2 + 1 \rangle
\]

Let \( i \) be image of \( X \) in the quotient. To check that \( i^2 = -1 \), let \( q : \mathbb{R}[X] \to \mathbb{R}[X]/\langle X^2 + 1 \rangle \) be the quotient homomorphism, and compute

\[
i^2 = q(X)^2 = q(X^2 + 1 - 1) = q(X^2 + 1) - q(1) = 0 - 1 = -1
\]

A polynomial ring in one variable \( k[X] \) over a field \( k \) is Euclidean in the sense that division-with-remainder produces a remainder with strictly smaller degree than the divisor. Thus, for any \( P(X) \in \mathbb{R}[X] \), there is a polynomial \( Q(X) \in \mathbb{R}[X] \) and \( a, b \in \mathbb{R} \) such that

\[
P(X) = Q(X) \cdot (X^2 + 1) + a + bX
\]

\[1\] In fact, the notion of polynomial (ring) itself, or variable or indeterminate \( X \), although familiar, require effort to make fully rigorous. Such rigor is not normally necessary or helpful, luckily.

1
Thus, every element of the quotient can be written as \(a + bi\) with \(a, b \in \mathbb{R}\).

\[
\begin{align*}
\text{real part of } a + bi & = \Re(a + bi) = \Re(a + bi) = a \\
\text{imaginary part of } a + bi & = \Im(a + bi) = \Im(a + bi) = b
\end{align*}
\]

The ring operations are inherited from the polynomial ring \(\mathbb{R}[X]\), so in \(\mathbb{C}\) multiplication and addition are associative, multiplication is commutative (as is addition), and multiplication and addition have the distributive property. More precisely, there is no \(\sqrt{-1}\) in \(\mathbb{R}\), so the (non-zero) ideal \(\langle X^2 + 1 \rangle\) is prime, hence maximal (being in a principal ideal domain), so the quotient is a field.

The other construction is inside the ring \(M_2(\mathbb{R})\) of two-by-two real matrices, by

\[
\begin{align*}
a + bi & \longleftrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{or} \quad a + bi \longleftrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix}
\end{align*}
\]

2. Addition, multiplication, conjugates, norms, metric

Using the representatives \(a + bi\), the addition inherited from the polynomial ring is identical to vector addition on ordered pairs of reals:

\[
(a + bi) + (c + di) = (a + c) + (b + d)i \quad \text{(for } a, b, c, d \in \mathbb{R})
\]

Multiplication inherits commutativity and associativity and distributivity (with respect to addition) from the polynomial ring. The formula for multiplication

\[
(a + bi) \cdot (c + di) = a \cdot c + a \cdot di + bi \cdot c + bi \cdot di = (ac - bd) + (ad + bc)i \quad \text{(since } i^2 = -1\text{)}
\]

has a geometric interpretation in terms of rotation and scaling, as follows. Using polar coordinates

\[
a + bi = r \cdot (\cos \alpha + i \sin \alpha) \quad c + di = R \cdot (\cos \beta + i \sin \beta)
\]

the product is

\[
(a + bi) \cdot (c + di) = r R \left( (\cos \alpha \cdot \cos \beta - \sin \alpha \cdot \sin \beta) + (\cos \alpha \cdot \sin \beta + \sin \alpha \cdot \cos \beta)i \right)
\]

\[
= r R \cdot \left( \cos(\alpha + \beta) + i \sin(\alpha + \beta) \right)
\]

by the addition formulas for sine and cosine. That is, the angles add, and the lengths multiply.

Any \(\mathbb{R}\)-linear ring homomorphism \(\varphi : \mathbb{C} \to \mathbb{C}\) must send a root of \(X^2 + 1 = 0\) to another root: \([2]\)

\[
\varphi(i)^2 + 1 = \varphi(i^2) + \varphi(1) = \varphi(0^2 + 1) = \varphi(0) = 0
\]

Thus, \(\varphi(i) = \pm i\). Thus, apart from the identity map \(\mathbb{C} \to \mathbb{C}\), there is at most one non-trivial (\(\mathbb{R}\)-linear) automorphism of \(\mathbb{C}\), the complex conjugation, often written as an over-bar:

\[
\overline{a + bi} = \overline{a + b \cdot i} = a + b(-i) = a - bi \quad \text{(for } a, b \in \mathbb{R}\text{)}
\]

\([2]\) Such a map sends \(0 \to 0\) and \(1 \to 1\): \(\varphi(0) + \varphi(z) = \varphi(0 + z) = \varphi(z)\), so \(\varphi(0)\) is still the additive identity, which is unique, so is 0; similarly, \(\varphi(1) \cdot \varphi(z) = \varphi(1 \cdot z) = \varphi(z)\), and \(\varphi(1)\) is still the multiplicative identity in the multiplicative group \(\mathbb{C}^\times\) of non-zero complex numbers.
To verify that complex conjugation is a ring homomorphism \( \mathbb{C} \to \mathbb{C} \), we could check directly, or invoke general results about field extensions. We give an explicit simplified form of a field-theory argument, as follows.

The map \( \mathbb{R}[X] \to \mathbb{R}[X] \) given by \( f(X) \to f(-X) \) is an \( \mathbb{R} \)-linear ring homomorphism, and stabilizes the ideal generated by \( X^2 + 1 \). Thus, this automorphism of \( \mathbb{R}[X] \) descends to the quotient \( \mathbb{C} = \mathbb{R}[X]/\langle X^2 + 1 \rangle \), giving complex conjugation.

Thus, without overtly checking, we have the multiplicativity of complex conjugation:

\[
\overline{(a + bi) \cdot (c + di)} = \overline{(a + bi)} \cdot \overline{(c + di)}
\]

Although it is helpful at the outset to write complex numbers in the form \( a + bi \), in fact there is no compulsion to separately identify the real and imaginary parts. Indeed, for many purposes it much better to use single characters to name complex numbers, as \( \alpha = a + bi \).

The real and imaginary parts are expressible via conjugation:

\[
\text{Re}(\alpha) = \frac{\alpha + \overline{\alpha}}{2}, \quad \text{Im}(\alpha) = \frac{\alpha - \overline{\alpha}}{2i}
\]

The complex norm or absolute value is

\[
|a + bi| = \sqrt{(a + bi) \cdot (a + bi)} = \sqrt{a^2 + b^2}
\]

Restricted to \( \mathbb{R} \subset \mathbb{C} \), this is the usual absolute value on \( \mathbb{R} \). Just as multiplication of complex numbers has a geometric sense, this norm coincides with the usual distance from \((0,0)\) to \((a,b)\) in \( \mathbb{R}^2 \). Thus, there is no ambiguity or inconsistency in declaring

\[
\text{distance from } a + bi \text{ to } c + di \text{ in } \mathbb{C} = \text{distance from } (a,b) \text{ to } (c,d) \text{ in } \mathbb{R}^2
\]

\[
= \left| (a + bi) - (c + di) \right| = \sqrt{(a - c)^2 + (b - d)^2}
\]

The multiplicativity of conjugation and of square root gives multiplicativity for the norm, again without overtly checking:

\[
|\alpha \cdot \beta| = |\alpha| \cdot |\beta| \quad \text{(for } \alpha, \beta \in \mathbb{C})
\]

Multiplicative inverses are expressible via norms and conjugates: for \( 0 \neq \alpha \in \mathbb{C} \),

\[
\frac{1}{\alpha} = \frac{\overline{\alpha}}{\overline{\alpha} \cdot \alpha} = \frac{\overline{\alpha}}{|\alpha|^2}
\]

---

[3] Here we use the characterization of polynomial rings \( k[X] \) as free commutative \( k \)-algebra on one generator, meaning that, for every commutative ring \( R \) containing \( k \) (and with \( 1_k = 1_R \) to avoid pathologies), for every \( r_0 \in R \) there is exactly one \( k \)-linear ring homomorphism \( k[X] \to R \) sending \( X \to r_0 \).

[4] This is the square root of the Galois norm.
3. Convergence of sequences and series, topology

Since the metric on $\mathbb{C}$ is identical to that on $\mathbb{R}^2$, questions about convergence of sequences or series of complex numbers immediately reduces to the same issue on $\mathbb{R}^2$. Namely, a sequence $\{\alpha_n : n = 1, 2, 3, \ldots\}$ of complex numbers converges to $\beta \in \mathbb{C}$ if and only if, for every $\varepsilon > 0$, there is $N$ such that, for all $n \geq N$, $|\alpha_n - \beta| < \varepsilon$.

A sequence $\{\alpha_n : n = 1, 2, 3, \ldots\}$ of complex numbers is a Cauchy sequence if, for every $\varepsilon > 0$, there is $N$ such that, for all $m, n \geq N$, $|\alpha_m - \alpha_n| < \varepsilon$. The completeness of $\mathbb{C}$ (or of $\mathbb{R}^2$) is that every Cauchy sequence converges.

The convergence of a sum $\sum_{n \geq 1} \alpha_n$ is characterized exactly by convergence of the sequence of its partial sums $\sum_{n \leq N} \alpha_n$. When this characterization is expanded, it is that, for every $\varepsilon > 0$, there is $N$ such that, for all $m, n \geq N$, $|\sum_{\ell<n} \alpha_\ell| < \varepsilon$.

A subset $U$ of $\mathbb{C}$ is open if, for every $z \in U$, there is an open ball $B = \{w \in \mathbb{C} : |z - w| < r\}$ of some positive radius $r$, centered at $z$, contained in $U$. The empty set and the whole $\mathbb{C}$ are both open.

A subset of $\mathbb{C}$ is closed if its complement is open.

A subset of $\mathbb{C}$ is bounded if it is contained in some ball of finite radius.

The best definition of compactness of a subset $K$ of $\mathbb{C}$ is that every open cover of $K$ admits a finite subcover, that is, for opens $\{U_\alpha\}$ such that $K \subset \bigcup_\alpha U_\alpha$, then there is a finite collection $U_{\alpha_1}, \ldots, U_{\alpha_n}$ such that $K \subset \bigcup_j U_{\alpha_j}$.

The classical equivalent of compactness is that the compact subsets of $\mathbb{C}$ (or $\mathbb{R}^n$) are exactly the closed, bounded subsets of $\mathbb{C}$.

Similarly, in $\mathbb{C}$ (or $\mathbb{R}^n$), sequential compactness of a set $K$ is that every sequence in $K$ has a convergent (to a point in $K$) subsequence. In $\mathbb{C}$ (or $\mathbb{R}^n$) sequential compactness and full compactness are demonstrably equivalent.

---

[5] There is a tradition of referring to infinite sums as series, to belabor the point that there is potentially a difficulty in adding up infinitely many things. However, in all other English usage sequence and series are exact synonyms, so the mathematical usage is difficult to endorse whole-heartedly.