Day 1: Two New Perspectives

Logistical comments:

- A bit of space is provided below each exercise for you to keep notes in. This will usually not be enough space to solve the problem — I recommend using your own paper to work on these problems, and only use the blanks to record key points.
- There are a lot of you! If you can't get to me (J-Lo) to ask about a question, **Gabrielle, Shiyue, Apurva, Kevin, Simran,** and **Andrew** have offered to help answer questions. (As a corollary of Rule 1, if they're teaching a different class, make sure the members of that class can ask their questions first!)
- Notation: $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers), $\mathbb{C}$ (complex numbers).

1.1 Perspective 1: Using More Numbers

Even if we only want to solve problems about integers or rational numbers, sometimes problems become much easier to solve if we allow ourselves to use other numbers in our calculations. For example:

Exercise 1.1. Find infinitely many integer solutions to Pell's Equation $a^2 - 2b^2 = 1$ by factoring the equation as a difference of squares.

This problem doesn't use much about these numbers besides knowing how to multiply them, but sometimes we want to use more interesting properties, like divisibility and prime factorization. Our goal is to study the properties of these new number systems.

Definition 1.2. *A subset $R \subseteq \mathbb{C}$ is a* ***subring of*** $\mathbb{C}$ *if it contains 0 and 1 and is closed under addition, subtraction, and multiplication; that is, if $a, b \in R$, then $a + b$, $a - b$, and ab are also in R.*

Definition 1.3. *A subset $R \subseteq \mathbb{C}$ is a* ***subfield of*** $\mathbb{C}$ *if it is a subring and if every nonzero element has a multiplicative inverse; that is, if $a \in R$ and $a \neq 0$, then $\frac{1}{a} \in R$.*

Example 1.4. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all subrings of $\mathbb{C}$. Of these, all but $\mathbb{Z}$ are subfields of $\mathbb{C}$.

We will create new subrings and subfields of $\mathbb{C}$ by starting with $\mathbb{Z}$ or $\mathbb{Q}$ and adding elements. The following exercise explains why this is a reasonable thing to do:

Exercise 1.5. Prove any subring of $\mathbb{C}$ contains $\mathbb{Z}$, and any subfield of $\mathbb{C}$ contains $\mathbb{Q}$.

Now if we just include extra elements at random, the result will almost certainly not be a subring of $\mathbb{C}$. In order to ensure the result is closed under addition, subtraction, and multiplication, we will have to add a very specific set of elements.

Definition 1.6. *If R is a subring of $\mathbb{C}$ and $\alpha \in \mathbb{C}$, then $R[\alpha]$ (pronounced "R **adjoin** α") is the set of complex numbers that can be written in the form $f(\alpha)$ for some polynomial $f(x)$ with coefficients in R.*

Example 1.7. Exercise 1.1 can be solved by working in $\mathbb{Z}[\sqrt{2}]$. The element $a + b\sqrt{2}$ can be written as $f(\sqrt{2})$, where $f(x) = a + bx$ is a polynomial with integer coefficients.

Exercise 1.8. Explicitly describe all the elements of (a) $\mathbb{R}[i]$, (b) $\mathbb{Z}[\frac{1}{3}]$, (c) $\mathbb{Q}[\sqrt[3]{5}]$, and (d) $\mathbb{Q}[\pi]$. Try to simplify each expression as much as possible.

Exercise 1.9. If R is a subring of $\mathbb{C}$ and $\alpha \in \mathbb{C}$, prove that $R[\alpha]$ is a subring of $\mathbb{C}$. (So yes, this process does actually make subrings!)

Exercise 1.10. Suppose R and S are subrings of $\mathbb{C}$, and S contains α and R. Prove that every element of $R[\alpha]$ is in S. (In particular, by Exercise 1.5, any subring of $\mathbb{C}$ that contains α will also contain $\mathbb{Z}[\alpha]$. We can interpret this as saying that $\mathbb{Z}[\alpha]$ is the *smallest* subring of $\mathbb{C}$ that contains α.)

1.2 Perspective 2: Sets of Multiples

There are a number of very nice properties of the natural numbers (primes, divisibility, GCDs, LCMs, factoring, etc) that we would like to explore in subrings of $\mathbb{C}$, but many of them will become considerably more complicated to work with in the process, because we won't have a good notion of "positive" to work with. Even in $\mathbb{Z}$ things aren't as nice as one might hope.

Exercise 1.11. Given integers m, n, we say $d \in \mathbb{Z}$ is a **greatest common divisor** of m and n if it is a common divisor (i.e. m and n are both integer multiples of d), and given any other common divisor e, d is an integer multiple of e. Show that every pair of nonzero integers has *more than one* greatest common divisor.

Exercise 1.12. Define what it means for an integer to be prime, and state precisely what it means for $\mathbb{Z}$ to have unique factorization into primes, *without* using ordering (so you can't mention natural numbers, positive/negative, inequalities).

The above exercises illustrate the (annoying) fact that there are distinct elements of $\mathbb{Z}$ which, from the perspective of divisibility, can't be told apart! They have the same factors and the same multiples. So instead of considering the individual elements, what if we instead studied the properties of their corresponding sets of multiples?

Definition 1.13. *Given an element a of a subring R of $\mathbb{C}$, the* ***set of multiples of*** *a, denoted (a), is $\{ar \mid r \in R\}$.*

Exercise 1.14. For each of the following situations, m, n, and a are integers. In each case, come up with an illustrative example (for example, $(-6) \subseteq (2)$ is an example for 1) and describe the relationship between integers that satisfy this relationship.

1. $(m) \subseteq (n)$.
2. $(m) = (n)$.
3. $(m) \cap (n) = (a)$.
4. $(m) \cup (n) = (a)$.
5. (a) is the set of all products of an element of (m) with an element of (n).
6. (a) is the set of all sums of an element of (m) with an element of (n).

Back to Perspective 1: Building Fields

We're going to start by building subfields of $\mathbb{C}$ by adjoining complex numbers to $\mathbb{Q}$. It turns out that some numbers (like $\sqrt{2}$ or i) are much nicer to adjoin then others.

Definition 1.15. *A complex number α is an* ***algebraic number*** *if it is the root of a monic rational polynomial; that is, for some polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_0, \ldots, c_{n-1} \in \mathbb{Q}$, we have $f(\alpha) = 0$.*

Exercise 1.16. Prove each of the following:[1]

1. α is algebraic if and only if $\frac{1}{\alpha}$ is in $\mathbb{Q}[\alpha]$.
2. α is algebraic if and only if $\mathbb{Q}[\alpha]$ is **finitely generated**. (*There exists a finite set $\beta_1, \ldots, \beta_n \in \mathbb{Q}[\alpha]$ (called a* ***generating set****) with the following property: given* any *$\gamma \in \mathbb{Q}[\alpha]$, we can find rational numbers $a_1, \ldots, a_n \in \mathbb{Q}$ that will let us write γ as $\gamma = a_1\beta_1 + \cdots + a_n\beta_n$.*)[2]
3. (Optional; challenge) α is algebraic if and only if $\mathbb{Q}[\alpha]$ is a subfield of $\mathbb{C}$.

[1] "if and only if" means you need to prove that each statement implies the other; this requires two proofs!

[2] This property might sound scary. Try to interpret it in the context of Exercise 1.8 (c) and (d). What are generating sets in each case?

Optional: Proving Bezout's Identities

The following claims will be needed later in the course (and in fact, they may be relevant for previous exercises). If you don't prove them, then you'll need to be willing to take them for granted.

Exercise 1.17. Let $m, n \in \mathbb{Z}$, and let d be a greatest common divisor. Prove that there exist integers a, b such that $am + bn = d$.

Exercise 1.18. Let $m(x), n(x)$ be polynomials with coefficients in some subfield F of $\mathbb{C}$, and let their greatest common divisor (also a polynomial with coefficients in F) be $d(x)$. Prove that there exist polynomials $a(x)$ and $b(x)$ with coefficients in F such that $a(x)m(x) + b(x)n(x) = d(x)$.

Optional: Further Exploration

Exercise 1.19. Repeat Exercise 1.1 but for the equation $a^2 - ab + b^2 = 1$. In particular, check that the factorization

$$a^2 - ab + b^2 = \left(a - b\frac{1+\sqrt{-3}}{2}\right)\left(a - b\frac{1-\sqrt{-3}}{2}\right)$$

holds, and that $a = 0, b = 1$ is a solution. How many solutions can be produced from this one?

Exercise 1.20. Repeat Exercise 1.1 but for the equation $a^2 - ab - b^2 = 1$. Describe the solutions $a, b \in \mathbb{Z}$ generated, and try to prove any patterns you find.

Exercise 1.21. (If you've learned about countable vs uncountable sets) Prove that there are countably many algebraic numbers. Conclude that there exist complex numbers that are not algebraic (these are called **transcendental**).