This is a sketch of the set-theoretic construction of models of the rational, real, and complex numbers.

In class we already talked about models of the natural numbers, i.e., sets satisfying the Dedekind-Peano axioms. Standard arguments show that between any two such sets there is a unique bijection taking 1 to 1 and "respecting the succesor operation." This fact should be interpreted as saying that from an abstract point of view, all such models are the same.[1]

Such models can be found within any infinite set, that is, a set S such that there is exists a map $\sigma\colon S \to S$ that is injective but not surjective. (The existence of an infinite set is essentially an axiom of set theory.) A subset $T \subset S$ is said to be *σ-stable* if $\sigma(T) \subset T$. In S, pick an element which is not in the image of σ, and call it 1. Then the intersection of all σ-stable subsets of S that contain 1 is a set that satisfies the Dedekind-Peano axioms.

Fix a model $\mathbb{N}$ of the natural numbers. For any ring R, there exists a unique map $f\colon \mathbb{N} \to R$ such that, with $\bar{n} := f(n)$, $\bar{1} = 1$ and $\overline{\sigma n} = \bar{n} + 1$ for all $n \in \mathbb{N}$. Using induction, one can show then that $\overline{m+n} = \bar{m} + \bar{n}$ and $\overline{mn} = \bar{m}\bar{n}$ for all $m, n \in \mathbb{N}$. (In these equations, everything on the left side under the overlines is in $\mathbb{N}$, and everything on the right side is in R.) We say that R *is a model of the integers* if:

(i) the map f is injective, and

(ii) for every $r \in R$, there exist $m, n \in \mathbb{N}$ such that $r = \bar{m} - \bar{n}$.

In class, we discussed a construction of such a model. Fix one, and call it $\mathbb{Z}$.

For any ring R the above map f extends uniquely to a *ring homomorphism* $g = g_R\colon \mathbb{Z} \to R$, i.e., a map such that $g(1) = 1$, $g(r+s) = g(r) + g(s)$ and $g(rs) = g(r)g(s)$. It follows that between any two models of the integers there is a bijective ring homomorphism—so they are abstractly the same.

Let F be a *field*. We say that F *is a model of the rational numbers* if, with $\bar{z} := g_F(z)$ for all $z \in \mathbb{Z}$,

(iii) the map g_F is injective, and

(iv) for every $r \in F$, there exist $m, n \in \mathbb{Z}$ such that $n \neq 0$ and $r = \bar{m}/\bar{n}$.

To construct such a model, define a relation $(p, q) \equiv (r, s)$ on pairs of integers whose second coordinate is nonzero to mean $ps = qr$; and check that this is an equivalence relation that is compatible with addition and multiplication. Denote the equivalence class of (p, q) by p/q. Define addition and multiplication of these equivalence classes by

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs}, \qquad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}.$$

Then check that the set $\mathbb{Q}$ of equivalence classes is a field. (The zero-element is $0/1$, the multiplicative identity is $1/1$, and when $p \neq 0$, the inverse of p/q is q/p.) The map $g_{\mathbb{Q}}$ is given by $g_{\mathbb{Q}}(z) = z/1$. And conditions (iii) and (iv) are easily verified. Thus $\mathbb{Q}$ is a model of the rationals.

If F is any field, the above map $g_F\colon \mathbb{Z} \to F$ extends uniquely to a ring homomorphism $h_F\colon \mathbb{Q} \to F$, and $h_F(p/q) = g_F(p)g_F(q)^{-1}$. As above, it follows that between any two models of the rationals, there exists a unique bijective ring homomorphism.

Any element of $\mathbb{Q}$ can be represented as p/q with $q > 0$ (because $r/s = (-r)/(-s)$). The field $\mathbb{Q}$ is an *ordered field*: it is totally ordered by the relation

$$p_1/q_1 < p_2/q_2 \iff p_1q_2 < p_2q_1 \qquad (q_1, q_2 > 0).$$

This order is compatible with addition and multiplication: for all $\alpha, \beta, \gamma \in \mathbb{Q}$, $\alpha < \beta \implies \alpha + \gamma < \beta + \gamma$ and, if $\gamma > 0$, $\alpha\gamma < \beta\gamma$.

[1] There are actually different "nonstandard" models which arise when you don't allow yourself to reason with arbitrary subsets of models. Explaining this would lead too far into the domain of mathematical logic for present purposes.

An ordered field is *complete* if every bounded-above subset has a least upper bound. There are numerous equivalent ways to express this condition, for example, *every Cauchy sequence has a limit.* (The terms here are defined just as they are in Analysis.) It can be shown that between any two complete ordered fields there is a unique order-preserving ring homomorphism. Thus from an abstract point of view, any two complete ordered fields are the same. They serve as models of the real numbers.

The ordered field $\mathbb{Q}$ can be embedded into a complete ordered field as follows: two Cauchy sequences (a_n) and (b_n) in $\mathbb{Q}$ are declared equivalent if for any $\epsilon > 0$ the absolute value $|a_n - b_n|$ is eventually (i.e., for all sufficiently large n, depending on ϵ) less than ϵ. This is an equivalence relation, compatible with termwise addition and multiplication of Cauchy sequences, and also with the order relation $(a_n) < (b_n) \iff$ there is an $\epsilon > 0$ such that a_n is eventually $< b_n - \epsilon$. It follows that the equivalence classes can be made into an ordered field, denoted $\mathbb{R}$; and one shows that $\mathbb{R}$ is complete. Details can be found in Landau's book (whose approach may be different, but essentially equivalent), or in many Analysis textbooks.

The embedding (i.e., injective order-preserving ring homomorphism) of $\mathbb{Q}$ into $\mathbb{R}$ is given by sending a rational r to the class of the constant Cauchy sequence $(r, r, r, \dots)$. The image of $\mathbb{Q}$ is dense in $\mathbb{R}$: every real number (i.e., member of $\mathbb{R}$) is the limit of a sequence of rational numbers.

Finally, the complex numbers should be a field $\mathbb{C}$ containing $\mathbb{R}$ and also an element i such that $i^2 = -1$ and such that every member of $\mathbb{C}$ can be represented in the form $a + bi$ with a and b in $\mathbb{R}$. Any two such fields $\mathbb{C}$ and $\mathbb{C}'$ can be shown to be related by a unique bijective ring homomorphism that takes i to i' and induces the identity map on $\mathbb{R}$ (which is a subfield of both $\mathbb{C}$ and $\mathbb{C}'$). Thus any two models of the complex numbers are abstractly the same.

One way to construct such a $\mathbb{C}$ is as the quotient ring $\mathbb{R}[X]/(X^2 + 1)$, which we will treat in the course.

Again, the construction in Landau is different but equivalent—necessarily so, in view of the foregoing uniqueness property of $\mathbb{C}$.