

The set F is a subset of the set of real numbers, where all the axioms for a field (the commutative and associative laws, etc.) are already satisfied. We simply need to observe that the sum and product of any two elements of F will again be elements of F ; then F will satisfy most of the axioms of a field just because \mathbf{R} does. (We say that F *inherits* these properties from \mathbf{R} .) We do also have to check that the special elements 0 and 1 lie in F (and they do). The fact that \mathbf{R} is a field means that every element of F has additive and multiplicative inverses somewhere in \mathbf{R} ; we just need to check that those inverses lie in F . Again, it's trivial that for every $z \in F$, the real number $-z$ is also in F , so we have only one thing left: to decide whether the multiplicative inverse of every $z \neq 0$ in F also lies in F .

When $a = \pi$ the answer is 'no'. Already $z = \pi$ itself is a nonzero element of F and so it has an inverse $1/\pi$ in \mathbf{R} , but this inverse is NOT in F . That is, $1/\pi$ cannot be written as a polynomial in π with rational coefficients. Indeed, if $1/\pi = c_0 + c_1\pi + c_2\pi^2 + \dots + c_n\pi^n$ then π would be a root of the polynomial

$$c_n X^{n+1} + c_{n-1} X^n + \dots + c_1 X^2 + c_0 X - 1$$

We could then clear denominators from the rational coefficients and get an integer polynomial whose root is π . That would make π be an algebraic number, which I assured you in class that it is not.

When $a = 5^{1/3}$, however, the answer is yes, and you can actually compute the inverse of any element of F , but really it's quicker (and more impressive!) to do this without much calculation. Indeed all you need is this fact:

F is a finite-dimensional vector space over \mathbf{Q}

(That means the axioms for a vector space are satisfied, where "scalar" means "element of \mathbf{Q} " rather than "element of \mathbf{R} ", which is the convention in Math 341.) I will leave it to you to think about those axioms and see F satisfies them. When $a = 5^{1/3}$, the finite-dimensionality of F comes from observing that F is spanned by $\{1, a, a^2\}$. (It's actually true that this set is also linearly independent, although that takes just a bit of work to actually prove, and we don't need to know it!)

Now here is the trick: if z is any single element of F , we may define a function $L_z : F \rightarrow F$ by the recipe $L_z(y) = zy$ for every element $y \in F$. (Make sure you understand this. For example, what is the corresponding function $L_i : \mathbf{C} \rightarrow \mathbf{C}$?). For each $z \in F$, this L_z is actually a *linear transformation*, since for every $y_1 \in F$, $y_2 \in F$, and $c \in \mathbf{Q}$ we have

$$L_z(y_1 + y_2) = L_z(y_1) + L_z(y_2) \quad \text{and} \quad L_z(cy_1) = cL_z(y_1)$$

simply because the distributive, associative, and commutative laws hold in \mathbf{R} .

Now if $z = 0$ then certainly L_z is the zero map and its kernel is all of F . But for any other $z \in F$, I claim $\ker(L_z) = \{0\}$. Indeed, if $L_z(y) = 0$, that would mean $zy = 0$, and since z is a nonzero real number, this forces $y = 0$.

But you had an important theorem in Linear Algebra: the condition $\ker(L_z) = \{0\}$ shows L_z to be an *invertible* linear map. (Perhaps you remember it this way: a square matrix with kernel= $\{0\}$ has an inverse.) In particular, L_z is also onto, that is, for every $w \in F$ the equation $L_z(y) = w$ has a solution for some $y \in F$. If we apply this in particular to the element $w = 1$ in F , we see that the equation $zy = 1$ has a solution for some $y \in F$, i.e. z has an inverse in F .

So we are done, and the only thing we used about a is that F is finite-dimensional over \mathbf{Q} . (If you want to make the proof constructive, and actually *compute* the inverse of an element $z \in F$, you could use the basis above to turn everything into some calculations with 3×3 matrices. The proof then hinges on whether the denominator involved, which is $\det(L_z)$, is nonzero. That denominator turns out to be $A^3 + 5B^3 + 25C^3 - 15ABC$ when $z = A + Ba + Ca^2$; you can show that there are no rational triples (A, B, C) for which this vanishes, except $(A, B, C) = (0, 0, 0)$, by considering the powers of 5 involved in A, B , and C .)

If you happen to know some Algebraic Number Theory, you can also compute the inverse of any nonzero element of F by noting $z \cdot z' \cdot z'' = N(z)$ where z' and z'' are the complex numbers obtained from z by replacing a by the other two complex cube roots of 5, and $N(z)$ is the same rational number that shows up as the determinant of L_z . It's not hard to show that z' and z'' must be nonzero as well, which makes $N(z)$ the product of three nonzero complex numbers and hence itself is nonzero, allowing us to divide by $N(z)$ to get $z^{-1} = z'z''/N(z)$.