For most people there mathematical career begins with calculus and the properties of the real numbers. The real numbers have many great properties. For example, we can add, multiple, and both of these operations behave nicely in that they are combinative, associative, and multiplication distributes over addition. However, the integers also have these things, but unlike the integers the real numbers have not only additive inverses, but also multiplicative inverses. For those of you have a course in analysis you might have learned that that the real numbers are what we call a field. Abstractly a field is a set $\mathbb{F}$ along with two binary operations $(+, \times)$, which we generally refer to as multiplication and addition such that $\forall a, b, c \in \mathbb{F}$:

\begin{enumerate}
\item $a + (b + c) = (a + b) + c$ \textbf{Associativity of Addition}
\item $a + 0 = 0 + a = a$ \textbf{Additive Identity}
\item $a + (-a) = (-a) + a = 0$ \textbf{Additive Inverses}
\item $a + b = b + a$ \textbf{Commutativity of Addition}
\item $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ \textbf{Associativity of Multiplication}
\item $a \cdot 1 = 1 \cdot a = 1, 1 \neq 0$ \textbf{Multiplicative Identity}
\item $a \cdot a^{-1} = a^{-1} \cdot a = 1$ \textbf{Multiplicative Inverses}
\item $a \cdot b = b \cdot a$ \textbf{Commutativity of Multiplication}
\item $a \cdot (b + c) = a \cdot b + a \cdot c$ \textbf{Distributive Law}
\end{enumerate}

As one notices a field carries with it a lot of structure, and the above axiomatic definition is somewhat unwieldily because of this. However, using the language we developed to talk about rings we can create a "nicer" definition of a field.

\textit{Date:} March 18, 2012.
Definition 1. A field $F$ is a commutative ring where every non-zero element has a multiplicative inverse.

A somewhat useful characterization of a field is that a field $F$ has only contains two ideals namely $(0)$ and $F$. This is easy to see since if $A \subset F$ is a non-zero ideal then $x \in A$, and since ideals are closed under multiplication $x^{-1}x = 1 \in A$, and so $A$ is intact $F$.

You are probably already quite familiar a number fields. For example, as mentioned above $\mathbb{R}$ is a field as is $\mathbb{C}$, and as is $\mathbb{Q}$. The rationals are actually a particularly type of field, namely $\mathbb{Q}$ is what we previously called the field of fractions of $\mathbb{Z}$. These are probably the most familiar fields and they have infinite in cardinality, however, there are many other more exotic fields, and even fields, which are finite in cardinality. For example, one can define

Definition 2. The characteristic of a field $F$ - denoted $\text{char}(F)$ - is the smallest natural number $p$ such that:

$$1 + \ldots + 1 = 0.$$ 

$p$ times

By convention if no such $p$ exists we say that $F$ has characteristic zero. The structure of a field means that the characteristic of a field is quite limited.

Proposition 1. The characteristic of a field $F$ is either zero or a prime number.

There are many ways to prove this, and we will present two of them here. The first prove will use contradiction, while the second one will use some slick ring theory that makes the convention of characteristic zero make sense.

Proof. Assume that characteristic of $F$ is not 0 and that $p$ is not prime so there exists $a, b \in \mathbb{Z}^+$ such that $p = ab$. Now by definition we know that:

$$0 = 1 + \ldots + 1 = p = ab$$ 

$p$ times

However, since $F$ is a field, and hence domain we know that $ab = 0$ means that either $a = 0$ or $b = 0$, and so:

$$1 + \ldots + 1 = 0 \quad \text{or} \quad 1 + \ldots + 1 = 0$$ 

$a$ times $b$ times

But, $a < p$ and $b < p$ contradicting the fact that $p$ is minimal, and so we see that $p$ cannot be composite. \qed

Proof. First let us recall that we have a unique ring homomorphism:

$$\mathbb{Z} \xrightarrow{\phi} F$$

$$n \mapsto 1 + \ldots + 1$$ 

$n$ times
Clearly the kernel of this map is generated by the characteristic of $F$. By the first isomorphism theorem for rings we know that we have the embedding:

$$\mathbb{Z}/\ker(\phi) \hookrightarrow F.$$  

Since $F$ is a field it is also a domain, and so $\mathbb{Z}/\ker(\phi)$ must also be a domain. However, we know that $\mathbb{Z}/\ker(\phi)$ is only a domain if $\ker(\phi)$ is a prime ideal. We have previously shown that the only prime ideals of $\mathbb{Z}$ are of the form $(p)$ where $p$ is prime or zero, and thus $\text{char}(F)$ is either prime or 0. □

At this point it might be helpful to see a few examples of fields and to determine their characteristic.

**Example 1.**

- Clearly $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ all have characteristic 0.
- The finite field of five elements $\mathbb{F}_5$ has characteristic 5.
- Since $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$ - this can be seen by noting that if it was reducible it would have a linear factor and then evaluate at 1 and 0 - we know that $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a finite field. Checking carefully it is fairly easy to see that this field has four elements in it, however, its characteristic is 2 since $1 + 1 = 0$ in $\mathbb{F}_2$.

These examples although interesting are in pretty simple, and there are many more exotic fields out here. Let us loot at two of such examples here:

**Example 2 (Example 1 Cont.).**

- Let us consider the field of fractions for the ring $\mathbb{F}_{17}[t]$, this is simply all rational functions over $\mathbb{F}_{17}$, and is usually denoted with rounded brackets instead of square, i.e.: $\mathbb{F}_{17}(t)$. Clearly this field is not finite since $\mathbb{F}_{17}[t] \subset \mathbb{F}_{17}(t)$ and $\mathbb{F}_{17}(t)$ is not finite. However, it has characteristic 17 since $\mathbb{F}_{17}$ has characteristic 17. So just because a field has finite characteristic it does not necessarily need to have finite order.

- Remember from our previous work with polynomials that we call a polynomial of the form $f_p = x^{p-1} + x^{p-2} + \ldots + 1$ where $p$ is prime a cyclotomic polynomial, and that these polynomials are intact irreducible over $\mathbb{Q}[x]$. So we can consider the field $\mathbb{Q}[x]/(f_p)$, which has characteristic zero, and infinite order. In fact this field is isomorphic to $\mathbb{Q}(\psi_p) \subset \mathbb{C}$ where $\mathbb{Q}(\psi_p)$ is the smallest field containing both $\mathbb{Q}$ and $\psi_p$ which is a $p$th root of unity. To see this we can create an explicit ring homomorphism by using an evaluation map:

$$\mathbb{Q}[x] \xrightarrow{x} \mathbb{Q}[\psi_p],$$

$$x \mapsto \psi_p.$$
The kernel of $\pi$ is in fact the ideal $(x^{p-1} + \ldots + 1)$ so by applying the first isomorphism theorem for rings we see that $\mathbb{Q}[x]/(f_p) \cong \mathbb{Q}(\psi_p)$. As interesting exploration into this field one could consider whether or not $\mathbb{Q}(\psi_p)$ is dense in $\mathbb{C}$.

So far in our explorations of algebra the general pattern has been that we define some algebraic structure e.g. a ring, a group, a module, and then we consider subsets of these objects like ideals, normal subgroups, submodules, and try and find interesting relationships about them. Fields are different in that the story of fields has been the story of polynomials. The evolution from the integers to the rational numbers to the reals, and finally to the complex numbers can be viewed as a quest to find solutions to polynomials. For example, it was the probably the ancients who discovered that the solution to a linear polynomial $ax - b$ is $b/a$, but $b/a$ is not always an integer. So why not throw in all these solutions to the integers so that we can always solve linear polynomials. Similarly the hunt for solutions of polynomials like $x^2 - 2$ and $x^2 + 1$ motivated the construction of the real and complex numbers respectively. So unlike many things in algebra instead of looking at smaller objects with fields we want to look at bigger extensions of fields because we often want for certain polynomials to have roots.

Given a field $K$ we say $K$ is a field extension of $F$ is $F$ is a subfield of $K$. Meaning that a $K$ is field extension of $F$ if and only if $K$ is an $F$-algebra. So for example $\mathbb{C}$ is a field extension of the reals, which themselves are a field extension of the rational numbers. Given a field extension it is natural to wonder if there is a way to tell how big the field extension is relative to the "base" field. To do this we shall define what we call the degree of a field extension:

**Definition 3.** If $K$ is a field extension of a field $F$ then the **degree** of a field extension - often denoted $\text{deg}(K/F)$ or $[K : F]$ - is the dimension of $K$ as an $F$ vector space.

Again it may beneficial to consider a examples of field extensions and to calculate their degree.

**Example 3.**

- If we consider $\mathbb{C}$ as a vector space over $\mathbb{R}$ we know that it has dimension two since $\{1, i\}$ form a basis for this space. Thus, $\mathbb{C}$ has degree 2 as a field extension of $\mathbb{R}$.

- If we consider $\mathbb{R}$ as a $\mathbb{Q}$-vector space we know we need an infinite number of vectors to span $\mathbb{R}$ since hitting the irrational numbers is very tough. Thus, as a field extension of $\mathbb{Q}$, $\mathbb{R}$ has infinite degree.

- Consider $\mathbb{Q}[x]/(x^2)$ as a field extension of $\mathbb{Q}$. Since $x^2$ is irreducible clearly this is field, and since it contains the constant polynomials it contains $\mathbb{Q}$ as a subfield. In addition, $\mathbb{Q}[x]/(x^2)$ is only contains polynomials of degree less than two so $\{1, x\}$ is a basis for $\mathbb{Q}[x]/(x^2)$ as a $\mathbb{Q}$-vector space.
As our last example might have hinted at if we have a field $F$ and extend it to $F[x]/(p)$ there should be a nice relationship between the degree of $p$ and the degree of the field extension. In fact this is precisely why we use the terminology degree of a field extension instead of using order or dimension.

**Proposition 2.** Let $F$ be a field and $p \in F[x]$ be an irreducible polynomial of degree $d$ then $F[x]/(p)$ is a field extension of $F$ of degree $d$.

**Proof.** Since $p$ is prime we know that $(p)$ is a maximal ideal since if it were not then $(p) \subset (a)$ and so $a$ would divide $p$ an thus $p$ would not be irreducible. Thus, $F[x]/(p)$ is in fact a field, and since it contains the constant polynomials $F$ is a subfield.

We now need to find a basis for $F[x]/(p)$ as a $F$-vector space. I claim that $\{1, x, \ldots, x^{d-1}\}$ is in fact a basis for this vector space. To see that these are linearly independent not that if $B(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{d-1} x^{d-1} = 0$ then $B(x)$ takes one the value zero infinitely many times. However, since $B(x)$ has degree $d - 1$ it can only take on zero $d - 1$ times unless all the $\lambda_i$’s are zero, and so these are linearly independent.

Now to show that these polynomials do in fact span $F[x]/(p)$ let $f \in F[x]$. By the division algorithm we know that $\exists q, r \in F[x]$ such that:
\[ f = pq + r \quad \text{deg}(r) < \text{deg}(p) \]

Thus, $f = r$, and since the degree of $r$ is less than $d$ clearly we can write using this basis. $\square$

**Definition 4.** Let $K$ be a field extension of $F$ then an element $\alpha \in K$ is algebraic over $F$ if an of the following equivalent statements are true:

- $\exists f \in F[x] - \{0\}$ such that $f(\alpha) = 0$.
- $[F(\alpha) : F]$ is finite.
- $F(\alpha) \cong F[x]/p$.

If $\alpha \in K$ does not satisfy any of these conditions we say that $\alpha$ is **transcendental** over $F$.

**Definition 5.** The unique monic polynomial satisfying either condition 1 or 3 of Definition 4 is the **minimal polynomial** of $\alpha$.

2. **Field Extensions - 3/9/12**

Some of the most famous problems in mathematics come from the geometers of ancient Greece. For example, geometers wondered whether or not one could using a compass and straightedge trisect an arbitrary angle, or square a circle. Many of these problems - such as the two mentioned previously - went unsolved for centuries, however, with the development of modern algebra and the emergence of Galois Theory these questions began to be answered. We will take more about compass and straightedge constructions later,
and eventually will get around to proving that you cannot in fact trisect or an arbitrary angle, or cube a circle. But in order to do this we must for the moment return to our discussion on field extensions.

Remember from last time that if we fix a field $\mathbb{F}$ we say $\mathbb{K}$ is a field extension if $\mathbb{K}$ is itself a field and $\mathbb{F}$ embeds into $\mathbb{K}$. Some examples of familiar field extensions are $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(i)$, and $\mathbb{Q} \subset \mathbb{R}$. Given a field extension $\mathbb{K}$ over $\mathbb{F}$ we defined its degree to be the dimension of $\mathbb{K}$ as a $\mathbb{F}$-vector space. So the degrees of the previous examples are 2, 2, and infinite respectively since we can use $\{1, i\}$ as a basis for both the first to extensions, while $\mathbb{R}$ as a $\mathbb{Q}$-vector space has infinite dimension.

Say we have $\alpha \in \mathbb{K}$ then another way to think about the degree of a field extension is to use the substitution principle to consider the unique ring homomorphism:

$$
\mathbb{F}[x] \xrightarrow{\phi} \mathbb{K}
$$

$$
x \mapsto \alpha
$$

$$
\lambda \mapsto \lambda \quad \text{if} \quad \lambda \in \mathbb{F}.
$$

If $\phi$ is injective then there is no polynomial $p \in \mathbb{F}[x]$ such that $p(\alpha) = 0$ meaning that $\alpha$ is transcendental. This means that $\mathbb{F}(x)$ and $\mathbb{F}(\alpha)$ are isomorphic as fields. So for example, since both $\pi$ and $e$ are transcendental $\mathbb{Q}(\pi) \cong \mathbb{Q}(x) \cong \mathbb{Q}(e)$ as fields. However, this does not mean that $\mathbb{Q}(e) = \mathbb{Q}(\pi)$ they are very different! They are only isomorphic as fields not as topological spaces since our map from $\mathbb{Q}(\pi)$ to $\mathbb{Q}(e)$ is not continuous. Note: $\mathbb{F}[\alpha]$ is not necessarily a ring, but if we take the field of fractions of $\mathbb{F}$ then it is and we denote this $\mathbb{F}(\alpha)$.

If on the other hand $\phi$ is not injective then $\phi$ has a non-trivial kernel, and since we are working PID we know that $\ker(\phi) = (p)$. Furthermore, since $\mathbb{F}[x]/(p)$ embeds in $\mathbb{K}$ we know that it is a domain and so $p$ must in fact be prime. With out loss of generality we can let $p$ be monic so that it is in fact unique. We then call $p$ the minimum polynomial $\alpha$ and know that:

$$
\mathbb{F}[x]/(p) \cong \mathbb{F}(\alpha) \quad \text{and} \quad [\mathbb{F}(\alpha) : \mathbb{F}] = \deg(p).
$$

In this case we say $\alpha$ is algebraic over $\mathbb{F}$. If every element of $\mathbb{K}$ is algebraic then we say $\mathbb{K}$ is algebraic over $\mathbb{F}$.

Now that we know we have an idea for what the degree of a field extension is one might question whether a field extension is algebraic if and only if it has finite degree. In order to answer this question we first will need s short, but incredibly useful proposition.

**Proposition 3.** Let $\mathbb{E}$ be a field extension of $\mathbb{F}$ and $\mathbb{K}$ be a field extension of $\mathbb{E}$ so that $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ then:

$$
[K : F] = [K : E][E : F].
$$
Proof. To prove this let $A = \{\alpha_1, \ldots, \alpha_n\}$ be a basis for $K$ over $E$, and $B = \{\beta_1, \ldots, \beta_m\}$ be a basis for $E$ over $F$. Taking $x \in K$ we know we can write:

$$x = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n.$$  

Since $A$ is a basis for $K$, since each $\lambda_i \in E$ we can rewrite this as:

$$x = (a_{i_1}\beta_1 + \cdots + a_{i_m}\beta_m)\alpha_1 + \cdots + (a_{n_1}\beta_1 + \cdots + a_{n_m}\beta_m)\alpha_n.$$  

Thus, the set $AB$ spans $K$ as an $F$-vector space. Since the $\lambda_i$’s uniquely determine the $a'_{i_j}$’s and the $\lambda_i$’s are themselves uniquely determined by $x$ we know that $AB$ must also be linearly independent. Thus, $AB$ is a basis of for $K$ as an $F$-vector space, and has dimension $mn$ so $[K:F] = mn$ exactly as we had wished. $\Box$

Now that we have that proposition let us consider the chain of field extensions:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[2^n]{2}) \subset \ldots.$$  

Since $(\sqrt[2^n]{2})^2 - 2 = 0$ clearly each one of these extension is algebraic. Furthermore, it is pretty easy to see that $\mathbb{Q}(\sqrt[2^n]{2})$ has a degree of 2 over $\mathbb{Q}(\sqrt{2(n-1)})$. Thus, we have an infinite chain of algebraic field extension, but applying the previous proposition we know that this results in a field extension of infinite degree. So clearly algebraic field extension need not have finite degree.

However, what about the other direction of our question? Are field extensions of a finite degree necessarily algebraic extensions? As it turns out this is the case.

**Proposition 4.** Let $\mathbb{K}$ be a field extension of $\mathbb{F}$ of finite degree then $\mathbb{K}$ is algebraic over $\mathbb{F}$.

**Proof.** Since $\mathbb{K}$ is a finite extension of $\mathbb{F}$ we know that as a $\mathbb{F}$-vector space $\mathbb{K}$ let $n$ be the dimension of $\mathbb{K}$ over $\mathbb{F}$. Now let $\alpha \in \mathbb{K}$ and consider the set:

$$A := \{1, \alpha, \alpha^2, \ldots, \alpha^n\}.$$  

Since $A$ has $n + 1$ elements in it and $\mathbb{K}$ only has dimension $n$ we know that this set must be linearly dependent over $F$. This means there exists $\lambda_i \in \mathbb{F}$ such that:

$$\lambda_n\alpha^n + \cdots + \lambda_0 = 0.$$  

However, this means that $\alpha$ satisfies $\lambda_nx^n + \cdots + \lambda_0$, and so $\alpha$ is in fact algebraic over $\mathbb{F}$. So we can conclude that $\mathbb{K}$ is in fact a algebraic field extension of $\mathbb{F}$. $\Box$

---

3. **Introduction to Constructions - 3/12/12**

Thinking back to high school some of you might remember learning compass and straight-edge constructions. For those of you who don’t remember give two points $p$ and $q$ we can construct:

- A line passing through $p$ and $q$. 

• A circle centered at $p$ passing through $q$ or a circle centered at $q$ passing through $p$.

These are the basic tools of construction, and from this we say that a point $\alpha$ is constructed if it the intersection of constructed lines or constructed circles.

As a historical aside one might wonder where this notion of construction comes from, and why it is relevant to the study of field extensions. In fact when these concepts did not originate in algebra, but instead come from us to the cult of Greek geometers. The ancient Greeks viewed numbers not in the formal modern sense, but instead as the lengths of line segments. So for them the goal of these constructions was to in fact "create" the numbers. Using these basic tools the Greeks were able to create numerous useful processes such as:

• Creating a line perpendicular to another line passing through a point.
• Creating a line parallel to another line passing through a point.
• Translating an certain line segment anywhere in Euclidean space.

We will not prove these, and instead leave them to the dedicated reader to prove. So the question now becomes using these contractions what numbers could the Greeks construct? If we let $p_0$ and $p_1$ be points in the Euclidean plane we can create a line $\ell_0$ through $p_0$ and $p_1$ and with out loss of generality can call the length of the line segment $|\overline{p_0p_1}|$ one. If we then create a circle centered at $p_1$ passing through $p_0$ we know that this circle will intersect $\ell_0$ at a point $p_2$ which is a distance 2 from $p_0$. So by repeating this procedure it is fairly obvious that we can construct all of the positive integers.

It is also possible to construct all the positive rational numbers. To see this agin let $p_0$ and $p_1$ be points in the plane and $\ell_0$ be the line throughout then, and say that the line segment $\overline{p_0p_1}$ has length one. Then let us construct to circles $C_1$ and $C_2$ about $p_0$ and $p_1$ respectively. These circles intersect at two points $q_0$ and $q_1$, and assuming you either proved the possibility of the above constructions, or simply believe us we can then construct a line $\ell_1$ which is perpendicular to $\ell_0$ and passes through $q_0$ and $q_1$. Let us call the intersection
the lines $\ell_1$ and $\ell_0$, $p_2$ then the line segment $\overline{p_0p_2}$ clearly has length 1/2. By inducting
upon this argument we see that we can obtain all rational numbers of the form $1/n$, and by
combining this construction with the one for the integers we see we can obtain the positive rational numbers.

![Diagram of constructing the rationals]

**Figure 2. Constructing the Rationals**

Now that we have constructed the positive rational numbers we might wonder whether we
can construct some irrational numbers, and if so which. Let $p_0$ and $p_1$ be points in
the Euclidean plane and let $\ell_0$ be the line determined by these points. Again let the line
segment $\overline{p_0p_1}$ have length one. Now let $C_1$ be the circle centered at $p_0$ and passing through
$p_1$. Now let us construct a line $\ell_1$ passing through $p_0$, which is perpendicular to the $\ell_0$.
Call the intersection points of $\ell_1$ and $C_1$, $p_2$ and $p_3$. Finally, let us construct the line $\ell_3$
passing through $p_1$ and $p_3$. We now have a line segment $\overline{p_1p_3}$ which is the hypotenuse of a
right triangle with legs of length 1, and so by the Pythagorean Theorem we can conclude
that $\overline{p_1p_3}$ has length $\sqrt{2}$.

By a similar method we can construct the square root of any constructible number. However,
can we construct every real number in this method, or even every algebraic number? In
order to answer this question we will need to jump forward in time a bit time till we have
the Cartesian plane. Once we have the idea of coordinates when we inductively construct
a chain of points:

$$\{p_0, p_1\} = \mathcal{P}_0 \subset \mathbb{Q}$$

$$\{p_2, p_1\} = \mathcal{P}_1 \subset \mathbb{P}_1$$

$$\{p_3, p_2\} = \mathcal{P}_2 \subset \mathbb{P}_2$$

This corresponds to a chain of field extensions:

$$K_0 \subset K_1 \subset \cdots$$

So for example if we choose $p_0 = (0, 0)$ and $p_1 = (1, 0)$ then $K_0 = \{p_0, p_1\} = \mathbb{Q}$ since $\mathbb{Q}$ in
$\mathbb{Q}$ is the smallest field contained in $\mathbb{R}$. If in the next stage we construct the point $(\frac{1}{2}, \sqrt{3})$
then we know that $K_1 = K_0(\frac{1}{2}, \sqrt{3})$ is equal to $\mathbb{Q}(\sqrt{3})$ since $\frac{1}{2} \in \mathbb{Q}$ and so we only need to
adjoin $\sqrt{3}$. With this in mind we will soon be able to prove that the only numbers that
are constructible number has degree $2^n$ over $\mathbb{Q}$. This means that many numbers are not
constructible and in fact many algebraic numbers are not constructible.
In the previous section we discussed how the ancient Greeks viewed numbers, and how they were able to construct numbers using compasses and straightedges. Recall that if $P$ be a collection of points in the Euclidean plane then we say that another point $p$ can be constructed in one step if from $P$ if:

- $p = \ell_1 \cap \ell_2$ where $\ell_2$ and $\ell_1$ are lines determined by $P$.
- $p \in \ell \cap C$ where $\ell$ is a line and $C$ is a circle determined by $P$.
- $p \in C_1 \cap C_2$ where $C_1$ and $C_2$ are circles determined by $P$.

The Greeks believed that starting from two points in the Euclidean plane and inductively using this type of construction they could "create" all numbers. Nowadays we know that this cannot be true since this would mean that the real numbers are countable, which we know is not the case.

Having discussed how the Greeks thought about numbers let us jump forward to the time of Descartes and consider these topics in a new way by introducing the Cartesian plane. After having chosen a coordinate system we can define:

**Definition 6.** The collection of points $P$ is defined over a field $\mathbb{K}$, where $\mathbb{K}$ is a subfield of $\mathbb{R}$, if $\forall p \in P \ p = (\alpha, \beta) \in \mathbb{R}$ and $\alpha, \beta \in \mathbb{K}$.

So for example, if we let $P = \mathbb{Q}^2$ then $P$ is obviously defined over $\mathbb{Q}$ since $\forall (\alpha, \beta) \in \mathbb{Q}^2$ by definition $\alpha, \beta \in \mathbb{Q}$. Or if we let $P = \{(0, \sqrt{35})$ then $P$ is defined over $\mathbb{Q}(\sqrt{35})$, since both $0$ and $\sqrt{35}$ are in $\mathbb{Q}(\sqrt{35})$. However, in this case $P$ is not defined over $\mathbb{Q}$ since $\sqrt{35}$ is not in $\sqrt{35}$. 

---

**Figure 3. Constructing the $\sqrt{2}$**

4. **Constructible Numbers - 3/14/12**

---
In the previous section we discussed how the Greeks left many famous open questions such as whether or not one can trisect an arbitrary angle, or whether you can square a circle. Having introduced the idea of what is for a collection of points to be defined over a field we can now begin to work towards answering these questions. In order to this we need a critical proposition.

**Proposition 5.** If \( \mathcal{P} \subset \mathbb{R}^2 \) is a collection of points defined over \( \mathbb{K} \) and \( q = (\alpha, \beta) \in \mathbb{R}^2 \) constructed in one step from \( \mathcal{P} \) then \( \alpha \) and \( \beta \) each satisfy some quadratic polynomial in \( \mathbb{K}[x] \).

So if we consider \( p_0 = (0, 0) \) and \( p_1 = (1, 0) \) we know that \( \mathcal{P} = \{p_0, p_1\} \) is defined over \( \mathbb{Q} \), and we can construct \((.5, -\sqrt{3}/2)\) is one step then we have the these points satisfy this polynomials:

\[
    x^2 - \frac{1}{4} \quad \text{and} \quad x^2 - \frac{3}{4}.
\]

Before we go about proving this proposition we need to prove a useful little lemma, which at its heart is something that people learn in high school geometry.

**Lemma 1.** If \( p, q \in \mathbb{R}^2 \) are distinct points defined over \( \mathbb{K} \) then:

1. The line through \( p \) and \( q \) has an equation with coefficients in \( \mathbb{K} \).
2. Both circles determined by \( p \) and \( q \) have equations with coefficients in \( \mathbb{K} \).

**Proof.** Let \( p = (\alpha, \beta) \) and \( q = (\gamma, \delta) \) where \( \{p, q\} \) is defined over \( \mathbb{K} \) meaning that \( \alpha, \beta, \gamma, \delta \in \mathbb{K} \). Now let us consider the two things we must prove starting by examining the line passing through \( p \) and \( q \).

1. First let us consider the case where \( \alpha = \gamma \). If this is the case then the line passing through \( p \) and \( q \) is vertical and so we know an equation for this line is \( x = \alpha \). Since \( \alpha \in \mathbb{K} \) we know in this case the lemma is true.

   Now let us consider the the case where \( \alpha \neq \gamma \). If this is the case we know that slope of the line passing through \( p \) and \( q \) is:

   \[
   \text{slope} = m = \frac{\delta - \beta}{\gamma - \alpha}.
   \]

   Since \( \mathbb{K} \) is a field we know that \( m \in \mathbb{K} \), and so when we write the equation for the line though \( p \) and \( q \):

   \[
   y = \frac{\delta - \beta}{\gamma - \alpha}(x - \alpha) + \beta.
   \]

   We see that the coefficients for the equations are in \( \mathbb{K} \) and so have proven the first part of the lemma.

2. Now let us turn our attention to the second part of the lemma and the equations for the circles determined by \( p \) and \( q \). These equations are:

   \[
   (x - \alpha)^2 + (y - \beta)^2 = r^2, \quad (x - \gamma)^2 + (y - \delta)^2 = r^2.
   \]
By how these circles are determined we can calculate the radius:

\[ r = \sqrt{(\alpha - \gamma)^2 + (\beta - \delta)^2}. \]

Thus, we see that the equations for the circles determined by \( p \) and \( q \) are:

\[
(x - \alpha)^2 + (y - \beta)^2 = (\alpha - \gamma)^2 + (\beta - \gamma)^2 \quad (x - \gamma)^2 + (y - \delta)^2 = (\alpha - \gamma)^2 + (\beta - \gamma)^2.
\]

Since \( K \) is a field it clear that the coefficients for these equations are in \( K \), and so the second part of the lemma also holds true.

\[ \square \]

Now that we have this lemma in hand we can turn our attention to proving the proposition.

**Proposition 5.** Let \( \mathcal{P} \subset \mathbb{R}^2 \) be defined over \( \mathbb{K} \) and let \( q = (\alpha, \beta) \) be constructed in 1 step from \( \mathcal{P} \). By how we defined construction earlier we know that this means \( q \) is one of three things:

1. Let \( q = \ell_1 \cap \ell_2 \) where \( \ell_1 \) and \( \ell_2 \) be lines determined by \( \mathcal{P} \). Then the equations for these lines can be written as:

\[ a_1x + b_1 = y \quad a_2x + b_2 = y. \]

Where since \( P \) is defined over \( \mathbb{K} \) by our lemma we know that coefficients of these equations are in \( \mathbb{K} \). Since \( q \) is the intersection of these lines we know that:

\[(a_1 - a_2)\alpha + (b_1 - b_2) = 0.\]

And so we know that \( \alpha \) is the solution to the polynomial \((a_1 - a_2)^2x^2 - (b_1 - b_2)^2\). Using a similar process we can see that \( \beta \) also solves a similar polynomial.

2. Now let us consider the case where \( q \) is the intersection of a line and a circle determined by \( \mathcal{P} \). Again applying we know that the equations for the line and circle are:

\[ y = mx + c \quad (x - a)^2 + (y - b)^2 = r^2. \]

Where thanks to our lemma all the coefficients are in \( \mathbb{K} \). Solving these equations for the intersection we know that:

\[(x - a)^2 + (mx + c - b)^2 - r^2 = 0.\]

Since \( \alpha \) is the interaction of these equations we know that it satisfies the above quadratic polynomial. Again, repeating the same process for \( y \) we can find a quadratic polynomial that is satisfied by \( \beta \).

3. Finally we have reached the last case we need to check. Namely when \( q \in C_1 \cap C_2 \) where \( C_1 \) and \( C_2 \) are circles determined by \( \mathcal{P} \). Again applying our lemma we know we can write the equations for these circles with coefficients in \( \mathbb{K} \).

\[
(x - a_1)^2 + (y - b_1)^2 = r_1^2 \quad (x - a_2)^2 + (y - b_2)^2 = r_2^2.
\]
Expanding and subtracting these equations we see that:

\((-2a_1 + 2a_2)x + (-2b_1 + 2b_2)y + (a_1^2 + b_1^2 - (a_2 + b_2)) = (r_1^2 - r_2^2)\).

So we see that we are left with the intersection of two lines, which we showed in the first case. Thus, we know that \(q\) is the solution to a quadratic polynomial.

So we see that as we wished a point is only constructible if its coordinates satisfy a degree two polynomial. \(\Box\)

If we start with two points in the Euclidean plane we are thus able to construct a lot more. We say that a point is constructible if we can construct a line segment whose length is that number. Constructible numbers are all the coordinates of the constructible points. Since each construction has degree of either 1, 2, or 4 we know that constructible numbers have degree \(2^n\) for some \(n\). With this in find we can finally prove one of the open problems we discussed in the last section. The Greeks wondered if it was possible to construct a square with the same area as a given circle. If we consider the unit circle we know that it has area \(\pi\), but to construct a square with are \(\pi\) we need to be able to construct a square with side length \(\sqrt{\pi}\). However, since \(\pi\) is transcendental, and thus \(\pi\) is not constructible, and so we cannot in fact square a circle.

![Figure 4. Squaring A Circle: Source: Wikipedia](image)

Another question we are now ready to tackle is whether given an arbitrary cube we can construct a cube with double the volume? If we start with a cube of which has side length 1 we want be able to construct a cube, which has volume 2. However, this would mean we need to construct sides of length \(\sqrt[3]{32}\), but since the minimum polynomial for \(\sqrt[3]{32}\) is \(x^3 - 2\), and so it does not have degree \(2^n\), and thus is not constructible. So just we square a circle we cannot double a cube.
5. Galois Theory - 3/16/12

Some of you might wonder why we have devoted so much time to going over constructions. Aside from the fact that they are interesting application of field extensions they give us a good motivation for our next topic - Galois Theory. Galois Theory arose out of the quest to find a general equation for 5th degree and higher polynomials. In order to begin our introduction into the subject we shall consider a few examples.

Let $f$ be a polynomial in $\mathbb{Q}[x]$. From previous work we know that $f$ factors completely into linear terms over $\mathbb{C}$.

$$ (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n). $$

However, $\mathbb{C}$ is much too big of field, and so instead let us consider $\mathbb{Q} \subset \mathbb{Q}(\lambda_1, \ldots, \lambda_n) \subset \mathbb{C}$. In this case we call $\mathbb{Q}(\lambda_1, \ldots, \lambda_n)$ the splitting field of $f$.

For example let us consider, $f(x) = x^4 - 4x^2 - 5$. Factoring $f$ over $\mathbb{C}$ we see that:

$$ f(x) = (x - \sqrt{5})(x + \sqrt{5})(x - i)(x + i). $$

Since $\sqrt{5}$ and $i$ are not elements of $\mathbb{Q}$ we know that the splitting field of $f$ is $\mathbb{Q}(\sqrt{5}, i)$. Since $\mathbb{Q}(\sqrt{5}, i)$ has degree four over $\mathbb{Q}$ we know $f$ has degree four.

We have seen that the degree is a very useful invariant of field, however, it does not necessarily tell us much about the field structure of the extension. Instead, it tells us more about the structure of our extension as a vector space, but it would be very useful to have a more subtle invariant of a field. One of Galois’s big contributions was the discovery of a more subtle invariant of a field called the Galois group. Before define the Galois Group we must first define what an $\mathbb{F}$-automorphism.

**Definition 7.** Given a field extension $\mathbb{F} \subset \mathbb{K}$, an $\mathbb{F}$-automorphism of the extension is $\phi : \mathbb{K} \rightarrow \mathbb{K}$ a field homomorphism which satisfies $\phi(\lambda) = \lambda$ for all $\lambda \in \mathbb{F}$.

Continuing our example from above if we let $f(x) = x^4 - 4x^2 - 5$ we can think about its $\mathbb{Q}$-automorphisms. Clearly, an obvious $\mathbb{Q}$-automorphism is the identity map:

$$ \phi : \mathbb{Q}(\sqrt{5}, i) \rightarrow (\sqrt{5}, i) $$

$$ x \mapsto x. $$

The question now becomes what are the other $\mathbb{Q}$-automorphisms. To answer this let us assume that $\phi$ is a $\mathbb{Q}$-automorphism and that $\phi(\sqrt{5}) = \alpha$. Using the fact that $\phi$ must be a homomorphism we know that:

$$ \phi(\sqrt{5}\sqrt{5}) = \phi(\sqrt{5})\phi(\sqrt{5}) = \alpha\alpha = \alpha^2. $$

Thus, since $\alpha^2 = 5$ we know we only have two choices for $\alpha$, namely $+\sqrt{5}$ and $-\sqrt{5}$. A similarly argument will show that $\phi(i)$ must be either $\pm i$, and so we have exactly four $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{5}, i)$. 

$$ \mathbb{Q}(\sqrt{5}, i) \rightarrow (\sqrt{5}, i) \quad \mathbb{Q}(\sqrt{5}, i) \rightarrow (\sqrt{5}, i). $$
\[ i \mapsto i \quad i \mapsto i. \]
\[ \sqrt{5} \mapsto \sqrt{5} \quad \sqrt{5} \mapsto -\sqrt{5}. \]

\[ \mathbb{Q}(\sqrt{5}, i) \xrightarrow{\mathbb{Q}} (\sqrt{5}, i) \quad \mathbb{Q}(\sqrt{5}, i) \xrightarrow{\mathbb{Q}} (\sqrt{5}, i). \]
\[ i \mapsto -i \quad i \mapsto -i. \]
\[ \sqrt{5} \mapsto \sqrt{5} \quad \sqrt{5} \mapsto -\sqrt{5}. \]

Checking the relations on these \( \mathbb{Q} \)-automorphisms under function composition we see that it is isomorphic to the Klein Four Group. This group of \( \mathbb{F} \)-automorphisms under function composition is exactly what we call the Galois Group of a field extension.

**Definition 8.** The **Galois Group** of a field extension \( \mathbb{F} \subset \mathbb{K} \) is the set of all \( \mathbb{F} \)-automorphisms of \( \mathbb{K} \) under function compositions.