# Chapter 5

# Field Extensions

In the history of mathematics there are several examples of constructions of objects that didn't exist until they were needed to solve problems. An example of this situation is related with what will be the main topic of this chapter.

Consider the natural numbers $\mathbb{N}$ and try to find the roots of the polynomial in $\mathbb{N}[x]$

$$p(x) = x + 2$$

Obviously, there is no natural number that when added 2 yields zero, thus it seems necessary to create a new class of numbers that would include the zero of $p(x)$. In this way we get the integers $\mathbb{Z}$. This set of numbers is much better than $\mathbb{N}$ in several aspects, one of them being the fact that $\mathbb{Z}$ is a ring and $\mathbb{N}$ is not. But even $\mathbb{Z}$ is not perfect, as the polynomial in $\mathbb{Z}[x]$

$$q(x) = 3x + 2$$

has no roots in $\mathbb{Z}$. Thus we need to create (or extend $\mathbb{Z}$ to) a new class of numbers that include the root of $q(x)$. In this way we come up with the rationals $\mathbb{Q}$. This set of numbers is even better than $\mathbb{Z}$ as, besides containing the roots of many polynomials that didn't have roots in $\mathbb{Z}$, it is a field and $\mathbb{Z}$ is not. However, it is easy to find polynomials in $\mathbb{Q}[x]$ (or even in $\mathbb{Z}[x]$!) that have no roots in $\mathbb{Q}$, an example would be

$$r(x) = x^2 - 2$$

Hence, we need yet a bigger class of numbers that contain these roots, thus we extend our set to the reals $\mathbb{R}$...

At this point a reflection, it seems that in the previous escalation of sets of numbers we went step by step, just adding what was necessary, but in the last step didn't we just add the roots that were missing in $\mathbb{Q}$ but also numbers like $\pi$ and $e$ that are not roots of polynomials! (this is not easy to prove). Maybe we went a little too far in the last step. Later in this chapter we will learn how to obtain exactly the right extension of $\mathbb{Q}$ that will contain just the 'missing roots'.

Anyway, let us continue with our analysis of roots of polynomials and sets of numbers. So far we are in the set of real numbers, but even here we can find polynomials in $\mathbb{R}[x]$ with no roots in $\mathbb{R}$, for instance

$$s(x) = x^2 + 1$$

thus we need to consider the complex numbers $\mathbb{C}$.

**Q:** When are we going to stop with this constant extension of numbers?!

**A:** No, because the fundamental theorem of algebra assures that all polynomials with coefficients in $\mathbb{C}$ must have all their roots in $\mathbb{C}$.

An interesting question is whether or not there are any fields "between" $\mathbb{R}$ and $\mathbb{C}$. As it is mentioned above, the step from $\mathbb{Q}$ to $\mathbb{R}$ seemed to be too big, the same may happen when we move from $\mathbb{R}$ to $\mathbb{C}$. Well, that is not the case.

But first a definition.

**Definition 28** *Let $E \subset F$ be fields such that the operations of $E$ are inherited from $F$ (same operations). Then we will say that $E$ is a subfield of $F$ and that $F$ is an extension of $E$.*

**Theorem 17** *$\mathbb{C}$ is the smallest extension of $\mathbb{R}$ containing $i$.*

**Proof.** Let $F$ be the smallest extension of $\mathbb{R}$ containing $i$. It is clear that $F \subset \mathbb{C}$.

Let $a, b \in \mathbb{R}$, then $a, b, i \in F$, by closure of multiplication in $F$ we get that $bi \in F$, and then by closure of the addition in $F$ we obtain

$$a + bi \in F \qquad \text{for all } a, b \in \mathbb{R}$$

which means that $\mathbb{C} \subset F$. ■

Let us try to 'complexificate' a field different from $\mathbb{R}$.

**Example 33** *Consider $i$ be an element (living in some place) such that $i^2 = -1$*

*Let $F = \mathbb{Z}_3$. It is easy to check that $F$ does not contain an element such that $x^2 = -1$. Consider,*

$$\mathbb{C}_3 = \{a + bi \ ; \ a, b \in F\}$$

*with the usual sum modulo 3 and a multiplication copied from the multiplication in $\mathbb{C}$ (just mod 3). Then it is not too hard to show that $\mathbb{C}_3$ is a field. In fact, the inverses are given by*

$$(a + bi)^{-1} = (a^2 + b^2)^{-1}(a - bi)$$

*familiar, huh?*

*Note that for $F = \mathbb{Z}_2$, this construction does not yield a new field, as $F$ contains an element such that $x^2 = -1$. On the contrary, the polynomial $p(x) = x^2 + 1$ is irreducible in both $\mathbb{R}[x]$ and $\mathbb{Z}_3[x]$ (considering $p(x)$ as an element of those rings).*

**Example 34** *Consider $F = \mathbb{Q}$, and let*

$$E = \{a + b\sqrt{5} \ ; \ a, b \in \mathbb{Q}\}$$

*Clearly $E$ contains $F$. It is also clear that $E$ is a commutative ring with one. Hence, the only thing left to prove (for $E$ to be an extension of $F$) is the existence of inverses for any non-zero element in $E$.*

*Let $\alpha = a + b\sqrt{5}$, then notice that*

$$(a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2 \in \mathbb{Q}$$

*thus*

$$(a + b\sqrt{5})\left(\frac{a - b\sqrt{5}}{a^2 - 5b^2}\right) = (a + b\sqrt{5})\left(\frac{a}{a^2 - 5b^2} - \frac{b}{a^2 - 5b^2}\sqrt{5}\right) = 1$$

*This extension is called $\mathbb{Q}(\sqrt{5})$.*

## Algebraic and transcendental elements

**Definition 29** *Let $\alpha$ be an element not in a field $F$, if $\alpha$ is a zero of some polynomial $p(x) \in F[x]$, then $\alpha$ is said to be algebraic over $F$, otherwise $\alpha$ is transcendental over $F$.*

*In the particular case that $\alpha$ is algebraic over $\mathbb{Q}$, we will say that $\alpha$ is an algebraic number.*

**Example 35**

*i* $\alpha = \sqrt{2}$ *is an algebraic number, as $\alpha$ is a zero of $p(x) = x^2 - 2 \in \mathbb{Q}[x]$.*

*ii* $\alpha = i$ *is algebraic over $\mathbb{R}$ (and $\mathbb{Q}$), as $\alpha$ is a zero of $p(x) = x^2 + 1 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$.*

*iii Let us check that the element $\alpha = 1 + i$ is an algebraic number. We use that if $\alpha$ is a zero of $p(x)$, then so is $\bar{\alpha}$. So we consider*

$$p(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - 2x + 2$$

*iv In $\mathbb{Z}_3$ consider an element $\alpha$ such that $\alpha^2 = 2$, this element cannot live in $\mathbb{Z}_3$, as the squares in $\mathbb{Z}_3$ are 0 and 1.*

*It is easy to show that $\alpha$ is a zero of $p(x) = x^2 - 2$, thus it is algebraic over $\mathbb{Z}_3$.*

Note that in the previous example there were elements that were shown to be algebraic over $\mathbb{Q}$ by using polynomials in $\mathbb{Z}[x]$. This is something we can always do, as the zeroes of $p(x)$ are the same as the zeroes of $Cp(x)$, for any constant $C$. However, we could still add some conditions on the polynomial used to make $\alpha$ an algebraic number.

**Definition 30** *Recall that a polynomial of degree $n$ such that the leading coefficient is equal to one is said to be monic.*

*An algebraic number that is a zero of a monic polynomial in $\mathbb{Z}[x]$ is said to be an algebraic integer.*

**Example 36** *The element $\alpha = \dfrac{-1+\sqrt{2}i}{3}$ is a zero of $p(x) = 3x^2 + 2x + 1$. Hence, $\alpha$ is an algebraic number but not an algebraic integer.*

**Remark 15** *So far we have examples of algebraic numbers but no examples of transcendental elements over $\mathbb{Q}$. This is because in order to show that $\alpha$ is transcendental over $\mathbb{Q}$ we need to show that there are no polynomials in $\mathbb{Q}[x]$ such that $p(\alpha) = 0$... and there are just too many polynomials to check!!*

*Arguably, the two most important transcendental elements over $\mathbb{Q}$ are $\pi$ and $e$. We will not give a proof for this fact but we will use it anyway.*

**Theorem 18** *Let $E$ be an extension of a field $F$, and let $\alpha \in E$ be algebraic over $F$. Then, there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.*

**Proof.** As $\alpha$ is algebraic, then there is a polynomial $q(x) \in F[x]$ such that $q(\alpha) = 0$. Among all the polynomials with this property, choose one with least degree, cal it $p(x)$.

Now let $a(x)$ be any polynomial such that $a(\alpha) = 0$, as $p(x)$ is minimal in degree, then we can use the division algorithm obtaining

$$a(x) = p(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } deg(r), deg(p)$$

but, as $a(\alpha) = p(\alpha) = 0$, then $r(\alpha) = 0$, thus implying that $r(x) = 0$. It follows that all polynomials having $\alpha$ as a zero are multiples of $p(x)$ and thus associates to it or factorable polynomials.

The monic part is done by dividing $p(x)$ by the coefficient with the largest exponent of $x$. ■

**Definition 31** *With the same notation as in the previous theorem*

*i The unique monic irreducible polynomial associated to $\alpha$ is called the minimal polynomial of $\alpha$ (relative to $F \subset E$). Most of the times we will denote it by $m_\alpha$.*

*ii If $p(x)$ is the minimal polynomial of both $\alpha$ and $\beta$, then we will say that $\alpha$ and $\beta$ are conjugates (definition inspired by the fact that if a complex number is a zero of a real polynomial, then so is its conjugate).*

**Remark 16** *The proof of the previous theorem tells us that if $p(\alpha) = 0$, then the minimal polynomial of $\alpha$ divides $p(x)$.*

**Example 37** *Let $\alpha = 1 + \sqrt{5}$. It is not so hard to check that $\alpha$ is a zero of $p(x) = x^2 - 2x - 4$.*

*If $p(x)$ were not $\alpha$'s minimal polynomial, then $m_\alpha$ would divide $p(x)$, implying that $\alpha \in \mathbb{Q}$, a contradiction. So, $p(x)$ is the minimal polynomial of $\alpha$.*

*The roots of $p(x)$ are $\alpha$ and $\beta = 1 - \sqrt{5}$. Hence, $\alpha$ and $\beta$ are conjugates. It is important to remark the resemblance between these conjugate elements and a pair of complex conjugate numbers.*

So far we have talked about algebraic elements, but we haven't learned anything about their sum or product, i.e. is the sum or product of algebraic elements algebraic? We are not ready yet to address this issue in all its generality, but at least we can start considering extensions containing only algebraic elements.

**Example 38** *Consider $\mathbb{C}$ as an extension of $\mathbb{R}$. It is easy to show that for any $\alpha \in \mathbb{C}$ there is a polynomial, for example,*

$$p(x) = (x-\alpha)(x-\bar{\alpha}) \ \in \mathbb{R}[x]$$

*that has $\alpha$ as a zero.*

*So, all elements in $\mathbb{C}$ are algebraic over $\mathbb{R}$.*

**Definition 32** *If every element of an extension $E$ of a field $F$ is algebraic over $F$, then $E$ is said to be an algebraic extension of $F$.*

In the previous example we showed that $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

**Example 39** *Consider $F = \mathbb{Q}$, and let*

$$E = \{a + b\sqrt{5} \ ; \ a, b \in \mathbb{Q}\}$$

*We know that $E$ is an extension of $F$. So, let us take an element $\alpha = a + b\sqrt{5}$ with $b \neq 0$ (i.e. $\alpha$ is not in $\mathbb{Q}$). We want to show that $\alpha$ is algebraic over $\mathbb{Q}$.*

*Mimicking what we did for complex numbers we consider*

$$[x - (a + b\sqrt{5})][x - (a - b\sqrt{5})] = x^2 - 2ax + (a^2 - 5b^2) \quad \in \mathbb{Q}[x]$$

*so, $\alpha$ is a zero of $p(x) = x^2 - 2ax + a^2 - 5b^2$. Hence, all elements in $E$ are algebraic over $\mathbb{Q}$, which means that $E$ is an algebraic extension of $\mathbb{Q}$.*

**Definition 33** *Let $F$ be a field, and $p(x)$ to be polynomial in $F[x]$. We define*

$$F[x]/(p) = \{q(x) + (p) \ ; \ q(x) \in F[x]\}$$

*where $q(x) + (p) = r(x) + (p)$, of and only if $q(x) - r(x)$ is a multiple of $p(x)$. In this case we will say that $q(x) = r(x)$ in $F[x]/(p)$.*

*That is, $F[x]/(p)$ is the set of polynomials modulo $p(x)$.*

It may be convenient, at least to create some intuition about $F[x]/(p)$, to think about the previous set as if it were $\mathbb{Z}_n$ (which is $\mathbb{Z}/(n)$, a set of numbers modulo $n$!!!).

So, as you can see, the similarities between $\mathbb{Z}$ and $F[x]$ do not stop showing up! Now we just need to check that $F[x]/(p)$ will be a ring (just like $\mathbb{Z}/(n)$) and that it would be a field depending on whether or not $p(x)$ is irreducible in $F[x]$ (the equivalent to being a prime number in $\mathbb{Z}$).

We would like to represent $F[x]/(p)$ in a similar way $\mathbb{Z}/(n)$ is represented. Most probably, you picture $\mathbb{Z}/(n)$ as the set of all positive numbers that are smaller than $n$. We now will see that something similar occurs with $F[x]/(p)$.

**Remark 17** *Let $p(x)$ be a polynomial in $F[x]$, we want to find a representation for $F[x]/(p)$.*

*Let $q(x) \in F[x]$ having degree larger or equal than the degree of $p(x)$, we use the division algorithm to get*

$$q(x) = p(x)d(x) + r(x)$$

*where $r(x) = 0$ or $deg(r) < deg(p)$.*

*Now note that $q(x) - r(x) = p(x)d(x)$, that is $q(x) + (p) = r(x) + (p)$.*

*It follows that we can represent the elements in $F[x]/(p)$ as the set of all polynomials in $F[x]$ with degree less than the degree of $p(x)$. We will say that $r(x)$ is the reduction modulo $p(x)$ of $q(x)$.*

*Also, note that $p(x)$ becomes $0$ in $F[x]/(p)$.*

We define two operations in $F[x]/(p)$. The sum of $q(x) + (p)$ and $r(x) + (p)$ (both in $\in F[x]/(p)$) is $s(x) + (p)$, where $s(x)$ is the reduction modulo $p(x)$ of $q(x) + r(x)$ (computed in $F[x]$). Similarly, the product of two elements in $F[x]/(p)$ is the reduction modulo $p(x)$ of their product in $F[x]$.

In exercise 10 you will show that if $p(x) \in F[x]$ is reducible in $F[x]$, then $F[x]/(p)$ has zero divisors, thus in this case $F[x]/(p)$ is not a field. The converse of this result is also true.

**Theorem 19 (Kronecker)** *Let $p(x) \in F[x]$ be irreducible in $F[x]$, then $F[x]/(p)$ is a field.*

**Proof.** Let $q(x) + (p)$ be a non-zero element of $F[x]/(p)$, we want to show that $q(x) + (p)$ has an inverse in $F[x]/(p)$.

Because of the analysis of the representatives of $q(x) + (p)$ done before, we can consider $q(x)$ to be a polynomial in $F[x]$ of degree less than the degree of $p(x)$. It follows that $gcd(p, q) = 1$, thus the Euclidean algorithm in $F[x]$ provides polynomials $\alpha(x), \beta(x) \in F[x]$ such that

$$\alpha(x)p(x) + \beta(x)q(x) = 1$$

It follows that $\alpha(x)p(x) = 1 - \beta(x)q(x)$, thus $1 + (p) = \beta(x)q(x) + (p)$. Hence,

$$[\beta(x) + (p)][q(x) + (p)] = 1 + (p)$$

which means that the inverse of $q(x) + (p)$ is $\beta(x) + (p)$. ■

**Remark 18** *As $E = F[x]/(p)$ contains the elements $f + (p)$ for all $f \in F$, then we can consider $F$ to be contained in $E$. Hence, if $p(x)$ is irreducible, we can consider $E$ to be a field extension of $F$.*

*Also, if $p(x) = a_0 + a_1x + \cdots + a_nx^n$ is an irreducible polynomial in $F[x]$, then*

$$p(y) = [a_0 + (p)] + [a_1 + (p)]y + \cdots + [a_n + (p)]y^n$$

*is a polynomial in $E[y]$. Now note that*

$$\begin{aligned} p(x + (p)) &= [a_0 + (p)] + [a_1 + (p)][x + (p)] + \cdots + [a_n + (p)][x + (p)]^n \\ &= a_0 + (p) + a_1x + (p) + \cdots + a_nx^n + (p) \\ &= p(x) + (p) \\ &= 0 + (p) \end{aligned}$$

*That is, $x + (p)$ is a root of $p(y)$. All this means that the polynomial $p(x)$ that was irreducible over $F[x]$ has a zero in E!!!*

Hence, we can always assume that any polynomial has a root in some field extension of $F$. The only problem is that the extension we found is hard to work with (and pretty ugly-looking), so we need a better representation for the elements in $F[x]/(p)$. In order to do this, we will use that $\alpha = x + (p)$ is a zero of $p$ in $F[x]/(p)$ and we will, sort of, do the inverse process we did before.

Let $p(x) \in F[x]$ be a polynomial of degree $n$ irreducible in $F[x]$. Let $\alpha$ be a zero of $p(x)$ in some extension $E$ of $F$ (we know we can do this because of the previous remark). As we want to construct a field (which we will call $F(\alpha)$) that is 'similar' to $F[x]/(p)$, then the elements in $F(\alpha)$ are represented by polynomials in $\alpha$ of degree less than $n$, that is

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \ ; \ a_i \in F \text{ for all } i\}$$

where the addition and multiplication in $F(\alpha)$ is given by not forgetting that $p(\alpha) = 0$ (that is equivalent to not forget in $F[x]/(p)$ $p$ was equal to zero). This condition, most of the times is something one does not need to keep track (too much), as we will probably know the element $\alpha$, so we should be able to operate with it with not much difficulty.

**Definition 34** *The extension $F(\alpha)$ is called the extension of $F$ by $\alpha$, or the extension obtained by adjoining $\alpha$ to $F$, or $F$-adjoined-$\alpha$.*

**Example 40** *Consider the extension of $\mathbb{Q}$ we called $\mathbb{Q}(\sqrt{5})$, and the extension $\mathbb{C}_3$ of $\mathbb{Z}_3$ that we learned about in examples 33 and 34.*

*It is easy to see that the new construction we have just learned yields those fields as $\mathbb{Q}$ adjoined $\sqrt{5}$ and $\mathbb{Z}_3$ adjoined $i$. Thus, $\mathbb{C}_3$ is now called $\mathbb{Z}_3(i)$.*

Now let us construct $\mathbb{Q}(3+4i)$, note that we don't know $m_{3+4i}(x)$. Actually, we don't even know whether or not $\alpha = 3+4i$ is algebraic over $\mathbb{Q}$. What we do know is that $\alpha$ is algebraic over $\mathbb{R}$.

As we have done before, we look for the minimal polynomial of $\alpha$ in $\mathbb{Q}[x]$ by using the conjugate of $\alpha$.

$$p(x) = (x-\alpha)(x-\bar{\alpha}) = (x-(3+4i))(x-(3-4i)) = x^2 - 6x + 25$$

which is in $\mathbb{Q}[x]$!!!!

Thus, we have found $m_{3+4i}(x)$ in $\mathbb{Q}[x]$. It follows that,

$$\mathbb{Q}(3+4i) = \{a + b(3+4i) \ ; \ a, b \in \mathbb{Q}\}$$

and the operations will use that $(3+4i)^2 = 6(3+4i) - 25$. For example,

$$\begin{aligned}
[5-7(3+4i)][2+(3+4i)] &= 10 + 5(3+4i) - 14(3+4i) - 7(3+4i)^2 \\
&= 10 - 9(3+4i) - 7(3+4i)^2 \\
&= 10 - 9(3+4i) - 7[6(3+4i) - 25] \\
&= 10 - 9(3+4i) - 42(3+4i) + 175 \\
&= 185 - 51(3+4i)
\end{aligned}$$

**Example 41** *Let us see a couple of examples we will probably see again during this semester.*

*i In order to construct $\mathbb{Q}(\sqrt[4]{2})$ we need the minimal polynomial of $\alpha = \sqrt[4]{2}$. As $\alpha^4 - 2 = 0$, then we know that $m_\alpha(x)$ divides $x^4 - 2$, but this polynomial is irreducible over $\mathbb{Q}$ because of Eisenstein's criterion. Thus $m_{\sqrt[4]{2}}(x) = x^4 - 2$. It follows that*

$$\mathbb{Q}(\sqrt[4]{2}) = \{a + b\sqrt[4]{2} + c(\sqrt[4]{2})^2 + d(\sqrt[4]{2})^3 \ ; \ a, b, c, d \in \mathbb{Q}\}$$

*The operations are computed using that $(\sqrt[4]{2})^4 = 2$, which is obvious!! So, in this case, the operations in $\mathbb{Q}(\sqrt[4]{2})$ follow naturally from the operations in $\mathbb{R}$.*

*ii Now consider $1 \neq \omega$, a $5^{th}$ root of unity, i.e. $\omega^5 = 1$, and construct $\mathbb{Q}[\omega]$.*

*As $\omega^5 - 1 = 0$, then we know that $m_\omega(x)$ divides $x^5 - 1$. We know this polynomial is reducible over $\mathbb{Q}$, as*

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$

*Now, as $\omega \neq 1$, then $\omega$ is a zero of $x^4 + x^3 + x^2 + x + 1$, which is irreducible!!!! Thus*

$$m_\omega(x) = x^4 + x^3 + x^2 + x + 1$$

*It follows that*

$$\mathbb{Q}(\omega) = \{a + b\omega + c\omega^2 + d\omega^3 \ ; \ a, b, c, d \in \mathbb{Q}\}$$

*The operations are computed using that $\omega^4 = -\omega^3 - \omega^2 - \omega - 1$.*

We have seen in the examples that all elements in an extension $E$, like the ones we have studied, look similar because the only thing that changes is the elements in the base field $F$ ($\mathbb{Q}$ in the previous examples). The set of elements that is invariant in the presentation of the elements in $E$ is called a basis of the extension over $F$. The number of elements in a basis is called the dimension of $E$ over $F$, and it is denoted $[E : F]$. For example,

1. In $\mathbb{Q}(\sqrt[4]{2})$, the basis over $\mathbb{Q}$ is $\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3\}$, and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.
2. In $\mathbb{Q}(\omega)$, the basis over $\mathbb{Q}$ is $\{1, \omega, \omega^2, \omega^3\}$, and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$.
3. In $\mathbb{Q}(\sqrt{5})$, the basis over $\mathbb{Q}$ is $\{1, \sqrt{5}\}$, and $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$.
4. In $\mathbb{Z}_3(i)$, the basis over $\mathbb{Z}_3$ is $\{1, i\}$, and $[\mathbb{Z}_3(i) : \mathbb{Z}_3] = 2$.

5. The basis of $\mathbb{C}$ over $\mathbb{R}$ is $\{1, i\}$, so $[\mathbb{C} : \mathbb{R}] = 2$.

**Remark 19** *What justifies the names 'basis' and 'dimension' is that an extension $E$ of $F$ can be considered as a vector space over $F$. So, the elements of the basis of $E$ over $F$ form a basis of $E$ as an $F$-vector space (linearly independent and generating set). Thus $[E : F]$ is the dimension of $E$ as an $F$-vector space.*

**Definition 35** *An extension $E$ of $F$ is said to be finite if $[E : F] < \infty$.*

**Theorem 20** *An extension $E = F(\alpha)$, where $\alpha$ is an algebraic element over $F$, is finite. Moreover, $[E : F]$ equals the degree of $m_\alpha(x) \in F[x]$.*

**Proof.** This follows immediately from the way we defined a basis of $E$ over $F$. ■

Now we want to extend a field using several algebraic elements. We could either adjoin one element after the other to create a chain of ascending (each one contained in the next) fields, or we could try to adjoin all these elements at the same time. These two processes are equivalent, but the latter may lead to confusions or mistakes as some redundancy is possible.

Let $\alpha$ be an element in $E$ that is algebraic over $F$. Assume that $m_\alpha(x)$ has degree $n$ and that $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a basis of $F(\alpha)$ . Now, for $\beta$ and algebraic element over $F(\alpha)$, we define $F(\alpha, \beta)$ as the extension of $F(\alpha)$ obtained by adjoining $\beta$.

Assume that $m_\beta(x) \in F(\alpha)[x]$ has degree $m$ and that $\{1, \beta, \beta^2, \cdots, \beta^{m-1}\}$ is a basis of $F(\alpha, \beta)$ over $F(\alpha)$. It follows that the elements in $F(\alpha, \beta)$ look like

$$f_0 + f_1\beta + f_2\beta^2 + \cdots + f_{n-1}\beta^{n-1} \qquad \text{where } f_i \in F(\alpha) \text{ for all } i$$

but, as each $f_i \in F(\alpha)$, then

$$f_i = a_{i0} + a_{i1}\alpha + a_{i2}\alpha^2 + \cdots + a_{i\ n-1}\alpha^{n-1} \qquad \text{where } a_{ij} \in F \text{ for all } i, j$$

It follows that $F(\alpha, \beta)$ could be consider as having basis

$$\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}, \beta, \beta\alpha, \beta\alpha^2, \cdots, \beta\alpha^{n-1}, \cdots\cdots, \beta^{m-1}, \beta^{m-1}\alpha, \beta^{m-1}\alpha^2, \cdots, \beta^{m-1}\alpha^{n-1}\}$$

over $F$. Don't forget the multiplication in $F(\alpha, \beta)$ will be given by the minimal polynomials of $\alpha$ and $\beta$.

we have just shown (only in a particular case, though)

**Theorem 21** *Let $F \subset K \subset E$ be fields, where $E$ is an extension of $F$ (and so is $K$), then*

$$[E : F] = [E : K][K : F]$$

**Remark 20** *Let $E$ be a finite extension of $F$ with $[E : F] = n$. Consider $\alpha \in E$, note that $F(\alpha)$ is a subfield of $E$. Hence, $[F(\alpha) : F]$ divides $[E : F]$. It follows that $\alpha$ is algebraic. Hence, if $E$ is a finite extension of $F$, then $E$ is an algebraic extension of $F$*

**Example 42** *Let us construct $E = \mathbb{Z}_3(\alpha, \beta)$, where $\alpha$ is a zero of $p(x) = x^2 + 1$ and $\beta$ is a zero of $q(x) = x^3 + x^2 + x + 2$. We know that*

$$\mathbb{Z}_3(\alpha) = \{a + b\alpha \ ; \ a, b \in \mathbb{Z}_3\}$$

*where $\alpha^2 + 1 = 0$, that is $\alpha^2 = 2$*

*Now we need to find the minimal polynomial of $\beta$ over $\mathbb{Z}_3(\alpha)$, we already know that $\beta$ satisfies $q(x) = x^3 + x^2 + x + 2$, but this polynomial (irreducible over $\mathbb{Z}_3$) could be reducible over $\mathbb{Z}_3(\alpha)$.*

*If $q(x)$ were reducible in $\mathbb{Z}_3(\alpha)[x]$ then the degree of $m_\beta(x) \in \mathbb{Z}_3(\alpha)[x]$ would be 2 or 1 (in case $\beta \in \mathbb{Z}_3(\alpha)$). But, as $\mathbb{Z}_3(\beta)$ is a subfield of $\mathbb{Z}_3(\alpha, \beta)$, and $q(x)$ is irreducible, then*

$$[\mathbb{Z}_3(\beta) : \mathbb{Z}_3] = 3$$

*and thus 3 divides $[\mathbb{Z}_3(\alpha, \beta) : \mathbb{Z}_3]$. It follows that $q(x)$ is irreducible in $\mathbb{Z}_3(\alpha)[x]$ and that $[\mathbb{Z}_3(\alpha, \beta) : \mathbb{Z}_3] = 6$.*

*Finally, the elements in $\mathbb{Z}_3(\alpha, \beta)$ look like*

$$\mathbb{Z}_3(\alpha, \beta) = \{a_0 + a_1\alpha + a_2\beta + a_3\alpha\beta + a_4\beta^2 + a_5\alpha\beta^2 \ ; \ a_i \in \mathbb{Z}_3\}$$

**Example 43** *We want to construct* $E = \mathbb{Q}(\sqrt{5}, \sqrt{3})$.

*It is easy to find the minimal polynomials of* $\sqrt{5}$ *and* $\sqrt{3}$ *over* $\mathbb{Q}$*, they are* $p(x) = x^2 - 5$ *and* $q(x) = x^2 - 3$ *respectively.*

*As* $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$*, then* $[E : \mathbb{Q}(\sqrt{5}, \sqrt{3})]$ *must be* 2 *or* 4*. If it is* 2 *then* $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{3})$*, which is not true because* $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$.

*It follows that* $[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}] = 4$ *and that*

$$E = \{a + b\sqrt{5} + c\sqrt{3} + d\sqrt{5}\sqrt{3} \ ; \ a, b, c, d \in \mathbb{Q}\}$$

*Also note that* $\mathbb{Q}(\sqrt{5}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.

If $\alpha$ is a transcendental element over $F$, then $F(\alpha)$ cannot have a finite basis over $F$, as the size of the basis depends on the degree of the minimal polynomial of $\alpha$, and $\alpha$ does not have one. In this case we say that

$$\{1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^n, \cdots\cdots\}$$

is a basis of $F(\alpha)$ over $F$. This makes sense because the elements in $F(\alpha)$ look like

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m$$

for some $m$ that can be as big as one wants. In this case we will also say that $[F(\alpha) : F] = \infty$.

**We will focus mostly on finite extensions, however do not forget that transcendental elements yield infinite extensions.**

**Theorem 22** *The set of algebraic elements over a field* $F$ *is a field.*

**Proof.** Let $\alpha, \beta$ be two algebraic elements over $F$, suppose that $[F(\alpha) : F] = n$ and that $[F(\beta) : F] = m$. Now construct $F(\alpha, \beta)$, it is easy to see that $[F(\alpha, \beta) : F] \leq nm$. So, all products, sums, inverses, etc of elements in $F(\alpha, \beta)$ are algebraic. ■

**Remark 21** *The previous theorem means that the set of all zeroes of all polynomials with coefficients in* $F$ *form a field. This field is called the algebraic closure of* $F$*. A field that is its own algebraic closure is said to be algebraically closed.*

*The fundamental theorem of algebra says that* $\mathbb{C}$ *is algebraically closed.*

**Remark 22** *Note that since a field* $F$ *is closed under addition, then* $n \cdot 1 = 1 + 1 + \cdots + 1$ *(*$n$ *times) is an element of* $F$ *for all* $n > 0$ *integer.*

*We define the characteristic of a field* $F$ *as the smallest positive integer* $n$ *such that* $n \cdot 1 = 0$*. If no such an* $n$ *exists, then we say the characteristic of* $F$ *is zero. We will write* $char(F)$ *for the characteristic of* $F$.

**Proposition 3** *Let* $F$ *be a field, then* $char(F)$ *is a prime number or zero.*

**Proof.** Assume $char(F) \neq 0$, then $char(F) = n$ for some positive integer $n$. Assume $n = ab$, then

$$0 = n \cdot 1 = (ab) \cdot 1 = (a \cdot 1)(b \cdot 1)$$

it follows that either $a \cdot 1 = 0$ or $b \cdot 1 = 0$. But as $char(F)$ is the smallest positive integer such that $n \cdot 1 = 0$, then either $a$ or $b$ must be $n$, so $n$ cannot be factored in a non-trivial way. ■

**Remark 23** *If* $char(F) = p$*, a prime number, then* $\mathbb{Z}_p \subset F$*. Similarly, if* $char(F) = 0$*, then* $\mathbb{Q} \subset F$.

## Splitting fields

We will dedicate just a little time to this very important concept, which is essentially what is behind the idea of constructing sets that contain just enough to have in them all roots of a given polynomial.

**Definition 36** *Let $F$ be a field, and $p(x) \in F[x]$, the splitting field of $p(x)$ over $F$ is the smallest field extension of $F$ that contains all zeroes of $p(x)$.*

**Example 44** *We have shown that $\mathbb{C}$ is the smallest field containing $\mathbb{R}$ and $i$, it follows that $\mathbb{C}$ is the splitting field of $p(x) = x^2 + 1$ over $\mathbb{R}$.*

*Similarly, $\mathbb{Q}(\sqrt{5})$ is the splitting field of $p(x) = x^2 - 5$ over $\mathbb{Q}$.*

**Remark 24** *If $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all the roots of $p(x) \in F[x]$, then $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ is a splitting field of $p(x)$ over $F$.*

**Example 45** *Let us find a splitting field over $\mathbb{Q}$ of $p(x) = x^4 - 8x^2 + 15 \in \mathbb{Q}[x]$.*

*We look for the zeroes of $p(x)$, so we try to factor it (in $\mathbb{C}$).*

$$x^4 - 8x^2 + 15 = (x^2 - 3)(x^2 - 5) = (x - \sqrt{3})(x + \sqrt{3})(x - \sqrt{5})(x + \sqrt{5})$$

*So, we need to adjoin $\pm\sqrt{3}$ and $\pm\sqrt{5}$ to $\mathbb{Q}$ to get the spitting field. But we notice that*

$$\mathbb{Q}(\pm\sqrt{3}, \pm\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

*So, the splitting field of $p(x)$ is $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, which is a field we have already discussed.*

**Remark 25** *Sometimes the splitting field may be found by adjoining elements that are not the zeroes of the polynomial. For instance, let $p(x) = x^2 + x + 1$.*

*We know the zeroes of $p(x)$ are*

$$\frac{-1 \pm \sqrt{3}i}{2} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{3}i$$

*So, as $\pm\frac{1}{2} \in \mathbb{Q}$, then the only elements we need to adjoin to $\mathbb{Q}$ to obtain the zeroes is $\alpha = \sqrt{3}i$.*

*It is clear that both zeroes of $p(x)$ live in $\mathbb{Q}(\alpha)$, thus $E \subset \mathbb{Q}(\alpha)$, where $E$ is the splitting field of $p(x)$ over $\mathbb{Q}$. Since $[\mathbb{Q}(\alpha)\mathbb{Q}] = 2$, then $E = \mathbb{Q}(\alpha)$.*

*Even though this construction seems longer and maybe cumbersome, it is better than just adjoining the zeroes of $p(x)$ because the presentation of the elements is nicer and multiplications are easier to compute.*

## Exercises

All these problems are interesting.

1. Prove all that is claimed in example 36.
2. Show that the golden ratio number $\varphi = (1+\sqrt{5})/2$ (related to all that it is beautiful, the Fibonacci sequence among other things) is algebraic over $\mathbb{Q}$.
3. Are the elements $\alpha = q + \pi$, where $q \in \mathbb{Q}$, transcendental over $\mathbb{Q}$? What about $\beta = qe$?
4. Prove all that is claimed in remark 16.
5. Let $E$ be an extension of $F$, and $\alpha \in E$ be algebraic. Define the annihilator of $\alpha$ in $F[x]$ by

$$Ann(\alpha) = \{p(x) \in F[x];\ p(\alpha) = 0\}$$

   Show that $Ann(\alpha)$ is a principal ideal of $F[x]$ and that it is generated by $m_\alpha$.

   What would be the annihilator of a transcendental element over $F$?
6. Prove in full detail that $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.
7. Show that if $\alpha$ is algebraic over $F$ then so is $p(\alpha)$ for all $p(x) \in F[x]$.
8. Find then minimal polynomial of $\alpha = \sqrt[3]{5}+7$ over $\mathbb{Q}$. Explain your method. Do you think this method would generalize to other algebraic elements over $\mathbb{Q}$? To ALL algebraic elements over $\mathbb{Q}$? Discuss.
9. Show that the operations defined for $F[x]/(p)$ do not depend on the choice of the representative in the elements in $F[x]/(p)$, that is, if

$$q(x) + (p) = r(x) + (p) \quad \textit{and} \quad a(x) + (p) = b(x) + (p)$$

   then

$$[q(x) + (p)] + [a(x) + (p)] = [r(x) + (p)] + [b(x) + (p)]$$

   and

$$[q(x) + (p)][a(x) + (p)] = [r(x) + (p)][b(x) + (p)]$$

10. Show that $\mathbb{Q}[x]/(p)$ is a commutative ring with one. Moreover, show that if $p(x)$ is reducible in $\mathbb{Q}[x]$, then $\mathbb{Q}[x]/(p)$ has zero divisors.
11. Let $p(x) = x^3 + 3x^2 - 7x + 11$ and $q(x) = x^4 + 5x^3 - 5x + 27$, both in $\mathbb{Q}[x]$.

    Find a polynomial $r(x) \in \mathbb{Q}[x]$ having degree less than 3 such that $q(x) = r(x)$ in $\mathbb{Q}[x]/(p)$. Now find another polynomial $s(x) \in \mathbb{Q}[x]$ having degree larger than 4 such that $q(x) = s(x)$ in $\mathbb{Q}[x]/(p)$.
12. Prove all that is claimed in example 40.
13. Show that $F(\alpha)$ is the smallest field extension of $F$ containing $\alpha$.
14. Show that if $a$ is an element in an extension $E$ of $F$ then $F(a)$ is a subfield of $E$.
15. Compute
    (a) $[3 - 5(\sqrt[4]{2})^2 + 7(\sqrt[4]{2})^3][2 - 4\sqrt[4]{2} + 6(\sqrt[4]{2})^3]$ in $\mathbb{Q}(\sqrt[4]{2})$
    (b) $[3 - 5\omega^2 + 7\omega^3][2 - 4\omega + 6\omega^3]$ in $\mathbb{Q}(\omega)$
16. Prove theorem 20 but using the standard linear algebra definitions of basis and dimension.
17. Construct $\mathbb{Z}_{11}(3 + 4i)$... does this set even make sense? Discuss.

18. Show that $[\mathbb{Q}(\sqrt[4]{18}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ but that $[\mathbb{Q}(\sqrt[4]{18}, \sqrt[4]{2}) : \mathbb{Q}] \neq 4 \cdot 4$... what is going on here? Discuss.

19. With the notation used in example 43.

    Compute $[1 + 2\sqrt{5} + 3\sqrt{3} + 3\sqrt{5}\sqrt{3}][4 + 3\sqrt{5} + 2\sqrt{3} + \sqrt{5}\sqrt{3}]$.

    Show that $\sqrt{15} \in E$. What can you say about $\mathbb{Q}(\sqrt{15})$ with respect to the extensions $E$, $\mathbb{Q}(\sqrt{5})$, and $\mathbb{Q}(\sqrt{3})$?

20. Show that if $[F(\alpha) : F] = n$, $[F(\beta) : F] = m$, and that $gcd(m, n) = 1$ then $[F(\alpha, \beta) : F] = nm$.

21. Show remark 23.

22. Assume that $p(\alpha) = 0$ and that $p(x) \in F[x]$ has degree two. Show that $F(\alpha)$ is a splitting field over $F$ of $p(x)$.

23. Show that every polynomial $p(x) \in F[x]$ has a splitting field over $F$.

24. Let $E$ be a splitting field over $F$ of $p(x) \in F[x]$. Assume the degree of $p(x)$ is $n$. How big can $[E : F]$ be?

25. Do both constructions of the splitting field in remark 25. Then multiply,

$$(1 - \sqrt{3}i)(2 + \sqrt{3}i)$$

    using the construction given( by adjoining $\sqrt{3}i$ to $\mathbb{Q}$), and then multiply

$$\left(1 - \frac{-1 + \sqrt{3}i}{2}\right)\left(2 + \frac{-1 + \sqrt{3}i}{2}\right)$$

    using the 'standard' construction of the splitting field ( by adjoining $\frac{-1+\sqrt{3}i}{2}$ to $\mathbb{Q}$).

26. Show that if $E$ is an extension of $F$, then $E$ is a vector space over $F$.

27. Let $p$ be a prime number. Find the minimal polynomial of a zero (different from 1) of $q(x) = x^p - 1$ over $\mathbb{Q}$.

28. Give an example of an algebraic number that is not an algebraic integer. Explain.

29. Find the minimal polynomial of $\alpha = \sqrt[4]{5}$ in $\mathbb{Q}[x]$. Repeat the problem using $\mathbb{Q}(\sqrt{5})$ instead of $\mathbb{Q}$.

30. Let $p(x) = x^2 + 2 \in \mathbb{Q}[x]$, and $\alpha$ a zero of $p(x)$. Find the inverse of $\alpha^9$ in $\mathbb{Q}(\alpha)$.

31. Write down the multiplication table for $\mathbb{Z}_2(\alpha)$, where $\alpha$ is a zero of $x^2 + x + 1$.

32. Is $\mathbb{Q}$ a field extension of $\mathbb{Z}_{11}$? Is $\mathbb{Z}_{22}$ a field extension of $\mathbb{Z}_{11}$? Is $\mathbb{Z}_{23}$ a field extension of $\mathbb{Z}_{11}$? Explain.

33. Show that $a + bi$ and $a - bi$ are conjugates in the sense of sharing their minimal polynomial in $\mathbb{Q}[x]$.

34. What is $\mathbb{Q}(\sqrt{5}) \cap \mathbb{Q}(\sqrt{3})$? Could it be possible that either $\mathbb{Q}(\sqrt{5})$ is an extension of $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{3})$ an extension of $\mathbb{Q}(\sqrt{5})$?

35. Is $\mathbb{R}$ an extension of $\mathbb{Q}(\sqrt{5})$? Is $\mathbb{C}$ an extension of $\mathbb{Q}(\sqrt{5})$?

36. Let $p(x)$ be an irreducible polynomial in $F[x]$. Assume its degree is two, then if $\alpha$ is a zero of $p(x)$ in some extension $E$ of $F$, then all zeroes of $p(x)$ live in $E$.

37. Let $\alpha$ be a zero of $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$, show that all zeroes of $p(x)$ live in $\mathbb{Z}_2(\alpha)$.

38. For the same $\alpha$ as above, how many elements does $F = \mathbb{Z}_2(\alpha)$ have?

    Repeat the previous problem for $E = \mathbb{Z}_3(\beta)$, where $\beta$ is a zero of the irreducible polynomial $q(x) = x^3 + x^2 + 2$.

39. Looking at the previous two problems. Claim what the size of $E = \mathbb{Z}_p(\alpha)$ is, where the degree of $m_\alpha(x)$ is $n$? Try to prove your claim.

40. Give a 'known' field that is equal to $F = \mathbb{R}(2i-1)$. Repeat the problem with $E = \mathbb{Q}(2-3\sqrt{5})$. Explain.

41. Find the splitting field of $p(x) = x^2 - x - 1$ over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{5})$.

42. Assume that every non-zero element $\alpha$ in a finite field $\mathbb{F}_q$ with $q$ elements satisfies $\alpha^{q-1} = 1$.
    What is the splitting field of $r(x) = x^q - x \in \mathbb{Z}_p[x]$ over $\mathbb{Z}_p$ if $q$ is a power of the prime $p$?