9. The k-th roots of unity.

Let k be a positive integer. We will discuss the roots of the polynomial $X^k - 1$. These roots are called k-th roots of unity, and of course they are algebraic over Q. They are an interesting set of numbers, and it will be useful to understand them. Fortunately, they are rather easy to understand. Recall from calculus the formula $e^{\varphi i} = (\cos \varphi) + (\sin \varphi)i$ (where φ is a real number). If you find $e^{\varphi i}$ on the complex plane, you will see that it is distance 1 away from the origin, (since $\sin^2\varphi + \cos^2\varphi = 1$) and the line connecting $e^{\varphi i}$ to the origin makes an angle of φ radians with the positive X-axis.

If we let $\varphi = 2\pi$, we get $e^{2\pi i} = (\cos 2\pi) + (\sin 2\pi)i = 1$. Now if n is an integer with $0 \leq n \leq k - 1$, then $e^{(n/k)2\pi i}$ raised to the k-th power gives $(e^{(n/k)2\pi i})^k = e^{n2\pi i} = (e^{2\pi i})^n = 1^n = 1$. Thus $e^{(n/k)2\pi i}$ is a k-th root of unity. Since the angles $(0/k)2\pi$, $(1/k)2\pi$, $(2/k)2\pi$, ... $(k-1/k)2\pi$ are all distinct, we see that $e^{(0/k)2\pi i}$, $e^{(1/k)2\pi i}$, ..., $e^{(k-1/k)2\pi i}$ are all distinct, and so constitute all of the k-th roots of unity (since $X^k - 1$ has k roots). If we graph these k k-th roots of unity, we find that they form the vertices of a regular k sided polygon centered at the origin.

(9.1) Exercise: On the complex plane, plot the roots of $X^5 - 1$ and $X^5 - 2$.

Suppose that we let $\omega = e^{(1/k)2\pi i} = (\cos 2\pi/k) + (\sin 2\pi/k)i$. We then see that $\omega^0 = 1, \omega^1 = \omega, \omega^2, \omega^3, \ldots, \omega^{k-1}$ are all of the k-th roots of unity. It is this fact, that every k-th root of unity is just some power of ω, which makes the k-th roots of unity so very user friendly. According to the next definition, ω is a primitive k-th root of unity.

Definition: A k-th root of unity β is called a primitive k-th root of unity if every k-th root of unity is equal to some power of β.

(9.2) Exercise: Determine for what values of n, $e^{(n/k)2\pi i}$ is a primitive k-th root of unity. (We have just seen that n = 1 always gives a primitive k-th root of unity, for any k. The other values of n which work depend upon what k is. You might want to inspect some particular choices of k before formulating and proving a general result.)

(9.3) Exertcise: Let ω be a primitive k-th root of unity. Show that for any field F, F[ω] contains all the m-th roots of unity, where m is any positive divisor of k.

(9.4) Exercises: Let $\alpha = a + bi$ and $\beta = c + di$ be in $\mathbf{C}$.

a) If $||\alpha|| = a^2 + b^2$, then $||\alpha||$ is the distance from α to the origin in the complex plane. Show that $||\alpha\beta|| = ||\alpha||||\beta||$.

b) Let $\angle\alpha$ be the angle between the positive X-axis and the straight line connecting α to the origin. Show that $\angle(\alpha\beta) = \angle\alpha + \angle\beta$. (Hint: Note that $\sin(\angle\alpha) = \frac{b}{a^2+b^2}$ and $\cos(\angle\alpha) = \frac{a}{a^2+b^2}$.)

c) Argue that by using parts (a) and (b), if you know where α and β are on the complex plane, then you can easily find where $\alpha\beta$ is on the complex plane.

d) Use the ideas presented in this exercise to give an alternate way of showing that the k k-th roots of unity form a regular k sided polygon centered at the origin.

10. Isomorphisms

Definitions: i) Let K and L be fields, and let $\Theta : K \to L$ be a function from K to L. Then Θ is called an isomorphism from K to L if Θ is one-to-one and onto, and if $\Theta(\alpha + \beta) = \Theta(\alpha) + \Theta(\beta)$ and $\Theta(\alpha\beta) = \Theta(\alpha)\Theta(\beta)$ for all $\alpha,\beta \in K$.

ii) Let K and L be fields, and let F be a field with $F \subseteq K \cap L$. Suppose that Θ is an isomorphism from K to L. If $\Theta|F$ is the identity function on F, then Θ is called an F-isomorphism from K to L. (Here, $\Theta|F$ denotes Θ restricted to F.)

iii) If K is a field, an automorphism of K is an isomorphism from K to itself.

iv) If $F \subseteq K$ are fields, an F-automorphism of K is an F-isomorphism of K to itself.

Example. Let K be a field. The identity function I, defined by $I(\alpha) = \alpha$ for all $\alpha \in K$, is an automorphsm of K, called the identity automorphism.

Example: For any complex number $\alpha = a + bi$ (with $a,b \in \mathbf{R}$), define $\Theta(\alpha) = a - bi$. We claim that Θ is an $\mathbf{R}$-automorphism of $\mathbf{C}$. We break this down into a series of exercises.

Remark: The automorphism mentioned above is particularly important, being useful in a lot of situations. It has been given the name "complex conjugation", or more simply, "conjugation". It is often denoted by an overbar. Thus, instead of writing $\Theta(\alpha)$, we write $\overline{\alpha}$, so that $\overline{a + bi} = a - bi$.

(10.1) Exercises: a) Show conjugation is one-to-one and onto.
b) Show that for all $\alpha,\beta \in \mathbf{C}$, $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, and $\overline{\alpha\beta} = (\overline{\alpha})(\overline{\beta})$.

c) Show that conjugation is the identity map on $\mathbf{R}$.

(10.2) Lemma: If Θ is an isomorphism from K to L, then $\Theta(0) = 0$.

Proof: $\Theta(0) = \Theta(0 + 0) = \Theta(0) + \Theta(0)$. Adding $-\Theta(0)$ to both sides gives $0 = \Theta(0)$.

(10.3) Exercises: Let Θ be an isomorphism from K to L.

a) Show that for $a,b \in K$, $\Theta(a - b) = \Theta(a) - \Theta(b)$, and, if $b \neq 0$, $\Theta(\frac{a}{b}) = \frac{\Theta(a)}{\Theta(b)}$. (Why does $b \neq 0$ imply $\Theta(b) \neq 0$?)

b) Show that $\Theta(1) = 1$.

b) Show that $\Theta|\mathbf{Q}$ is the identity on $\mathbf{Q}$ (so that Θ is automatically a $\mathbf{Q}$-isomorphism).

(10.4) Exercise: Let $F \subseteq K$ be fields, and let Θ be an F-automorphism of K. Define a function $\phi : K \to K$ as follows. For any $\alpha \in K$, since Θ is one-to-one and onto, there is a unique element $\beta \in K$ such that $\Theta(\beta) = \alpha$. Let $\phi(\alpha) = \beta$. Show that ϕ is an F-automorphism of K such that the two composition functions $\Theta \circ \phi$ and $\phi \circ \Theta$ both equal the identity automorphism I, and that no other F-automorphism of K has that property. (We will call ϕ the inverse of Θ, and write $\phi = \Theta^{-1}$.)

(10.5) Exercise: We know that conjugation is an $\mathbf{R}$-automorphism of $\mathbf{C}$. With terminology as in the previous exercise, show that conjugation is its own inverse.

We state an important theorem.

(10.6) Theorem: Let F be a field. Let g(X) be an irreducible polynomial in F[X], and let α and β be roots of g(X). Then there is a unique F-isomorphism Θ from $F[\alpha]$ to $F[\beta]$, such that $\Theta(\alpha) = \beta$.

Proof: We may assume that g(X) is monic. Note that Exercise (8.2)(d) shows that g(X) is the minimal polynomial of both α and β over F. Any element of $F[\alpha]$ can be expressed as $f(\alpha)$ with $f(X) \in F[X]$. Define $\Theta(f(\alpha))$ to be $f(\beta)$. Suppose that $f_1(X)$ and $f_2(X)$ are in F[X]. Using Exercise (8.2)(c), we see that $f_1(\alpha) = f_2(\alpha)$ iff α is a root of $f_1(X) - f_2(X)$ iff g(X) divides $f_1(X) - f_2(X)$ iff β is a root of $f_1(X) - f_2(X)$ iff $f_1(\beta) = f_2(\beta)$. This shows that Θ is both well defined and one-to-one. Since every element of $F[\beta]$ has the form $f(\beta)$ for some $f(X) \in F[X]$, clearly Θ is onto. Now for $f(\alpha)$ and $g(\alpha)$ in $F[\alpha]$, we have $\Theta(f(\alpha) + g(\alpha)) = \Theta((f + g)(\alpha)) = (f + g)(\beta) = f(\beta) + g(\beta) = \Theta(f(\alpha)) + \Theta(g(\alpha))$. Similarly, we see that $\Theta(f(\alpha)g(\alpha)) = \Theta(f(\alpha))\Theta(g(\alpha))$. Thus Θ is an isomorphism from $F[\alpha]$ to $F[\beta]$. Now let $c \in F$. Consider the constant polynomial $f(X) = c$. Thus $f(\alpha)$ and $f(\beta)$ both equal c. However, by definition of Θ, $\Theta(c) = \Theta(f(\alpha)) = f(\beta) = c$. Therefore, $\Theta|F$ is the identity on F, so

that Θ is an F-isomorphism. Next, let $f(X) = X$. Then by definition, $\Theta(f(\alpha)) = f(\beta) = b$. But $f(\alpha) = \alpha$, so that $\Theta(\alpha) = \beta$, as desired. This shows that Θ is a F-isomorphism from $F[\alpha]$ to $F[\beta]$ such that $\Theta(\alpha) = \beta$. Finally, we must show that Θ is unique. Therefore, suppose that Φ is also an F-isomorphism from $F[\alpha]$ to $F[\beta]$ with $\phi(\alpha) = \beta$. We must show that $\Theta = \Phi$. Consider any $f(\alpha) \in F[\alpha]$. Suppose that

$f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0$.

Now $\phi(f(\alpha)) =$

$\phi(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0) =$

$\phi(a_n\alpha^n) + \phi(a_{n-1}\alpha^{n-1}) + \ldots + \phi(a_0) =$

$\phi(a_n)\phi(\alpha)^n + \phi(a_{n-1})\phi(\alpha)^{n-1} + \ldots + \phi(a_0) =$

$a_n\phi(\alpha)^n + a_{n-1}\phi(\alpha)^{n-1} + \ldots + a_0 =$

$a_n\beta^n + a_{n-1}\beta^{n-1} + \ldots + a_0 = f(\beta) = \Theta(f(\alpha))$. Therefore, we see that $\phi(f(\alpha)) = \Theta(f(\alpha))$ for all elements $f(\alpha) \in F[\alpha]$. This shows that $\phi = \Theta$.

Example: Let $\alpha = \sqrt[3]{2}$, and let $\beta = \alpha\omega$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,i$. Since ω is a cube root of unity, we see that α and β are both roots of the polynomial $X^3 - 2 \in \mathbf{Q}[X]$, (which Eseinstein's Criterion shows is irreducible). Theorem (10.6) tells us that there is a unique $\mathbf{Q}$-isomorphism Θ from $\mathbf{Q}[\alpha]$ to $\mathbf{Q}[\beta]$ which carries α to β. (It is interesting to note that $\mathbf{Q}[\alpha] \subseteq \mathbf{R}$ while $\mathbf{Q}[\beta] \not\subseteq \mathbf{R}$.) By Theorem (8.7), we know that every element in $\mathbf{Q}[\alpha]$ can be expressed uniquely as $a_0 + a_1\alpha + a_2\alpha^2$, with

a_0, a_1, and a_2 in $\mathbf{Q}$. The definition of Θ given in the proof of Theorem (10.6) shows that $\Theta(a_0 + a_1\alpha + a_2\alpha^2) = a_0 + a_1\beta + a_2\beta^2$.

(10.7) Exercise: Discuss what Theorem (10.6) says in the case that $F = \mathbf{Q}$ and $g(X) = X^2 + 1$.

Example: Let $\alpha = \sqrt[3]{2}$, and $\beta = \sqrt[3]{3}$. It might be tempting to try to define a $\mathbf{Q}$-isomorphism Θ from $\mathbf{Q}[\alpha]$ to $\mathbf{Q}[\beta]$ by letting $\Theta(f(\alpha)) = f(\beta)$ for all $f(X) \in \mathbf{Q}[X]$. This does not work. Here is the problem. We have $\alpha^3 = 2$. Thus we would need $\beta^3 = (\Theta(\alpha))^3 = \Theta(\alpha^3) = \Theta(2) = 2$. However, $\beta^3 \neq 2$. Let us look at this from a slightly different viewpoint. We claim that the problem is that Θ is not well-defined (and so does not really exist). Specifically, let $f(X) = X^3$ and $g(X) = 2$. Then $f(\alpha) = \alpha^3 = 2 = g(\alpha)$. If Θ were well-defined, we would have $\Theta(f(\alpha)) = \Theta(g(\alpha))$. But $\Theta(f(\alpha)) = \Theta(\alpha^3) = (\Theta(\alpha))^3 = \beta^3$, and $\Theta(g(\alpha)) = \Theta(2) = 2$. Since $\beta^3 \neq 2$, Θ is not well-defined. Note that the minimal polynomial of α over $\mathbf{Q}$ is $X^3 - 2$, while the minimal polynomial of β over $\mathbf{Q}$ is $X^3 - 3$. That is why Θ is not well-defined. (As the proof of theorem (10.6) shows, in situations where α and β do have the same minimal polynomial over $\mathbf{Q}$, well-definedness is automatic, since that minimal polynomial is irreducible.)

We will need a theorem which is similar to, but a bit stronger than Theorem (10.6). We first must introduce a new (but easy) idea. Let $\Theta : K \to L$ be an isomorphism. We will use Θ to build a funcion from K[X] to L[X]. This new function will be so closely related to Θ that we will also call it Θ. Specifically, for $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$, we define $\Theta(f(X)$ to be $\Theta(f(X)) = \Theta(a_n)X^n + \Theta(a_{n-1})X^{n-1} + \ldots + \Theta(a_0)$. Note that $\Theta(f(X)) \in L[X]$.

Example: Let $\Theta : \mathbf{C} \to \mathbf{C}$ be conjugation, so that $\Theta(a + bi) = a - bi$, for $a,b \in \mathbf{R}$. If f(X) is the polynomial $(2 + 3i)X^3 - (\frac{3}{2} - 4i)X^2 + (\pi + 5i)X - (5 - 7i)$ in $\mathbf{C}[X]$, then the function $\Theta : \mathbf{C}[X] \to \mathbf{C}[X]$ described above is such that

$\Theta(f(x)) = (\Theta(2 + 3i))X^3 - (\Theta(\frac{3}{2} - 4i))X^2 + (\Theta(\pi + 5i))X - (\Theta(5 - 7i))$

$= (2 - 3i)X^3 - (\frac{3}{2} + 4i)X^2 + (\pi - 5i)X - (5 + 7i)$.

(10.8) Exercises: Let $\Theta : K \to L$ be an isomorphism.

a) Show $\Theta : K[X] \to L[X]$ is one-to-one and onto.

b) Show that for f(X) and g(X) in K[X], $\Theta(f(X) + g(X)) = \Theta(f(X)) + \Theta(g(X))$, and $\Theta(f(X)g(X)) = \Theta(f(X))\Theta(g(X))$.

c) Show that if f(X) is irreducible in K[X], then $\Theta(f(X))$ is irreducible in L[X].

Remark: Those readers familiar with ring theory will see that parts (a) and (b) say that $\Theta : K[X] \to L[X]$ is a ring isomorphism.

We now strengthen Theorem (10.6). The proof of the following result is very similar to the proof of Theorem (10.6), so we shall only start it, and leave many of the final details to the reader.

(10.9) Theorem: Let K and L be fields, and let $\Theta : K \to L$ be an isomorphism. Let $g(X)$ be an irreducible polynomial in $K[X]$ (so that $\Theta(g(X))$ is irreducible in $L[X]$). Let α and β be roots of $g(X)$ and $\Theta(g(X))$ respectively. Then there is a unique isomorphism $\Phi : K[\alpha] \to L[\beta]$, such that $\Phi(\alpha) = \beta$ and such that $\Phi|K = \Theta$.

Proof: Any element of $K[\alpha]$ can be expressed as $f(\alpha)$ with $f(X) \in K[X]$. Define $\Phi(f(\alpha))$ to be $h(\beta)$, where $h(X) = \Theta(f(X))$. Suppose that $f_1(X)$ and $f_2(X)$ are in $K[X]$, and that $\Theta(f_i(X)) = h_i(X)$, $i = 1,2$. We see that $f_1(\alpha) = f_2(\alpha)$ iff α is a root of $f_1(X) - f_2(X)$ iff $g(X)$ divides $f_1(X) - f_2(X)$ iff $\Theta(g(X))$ divides $\Theta(f_1(X) - f_2(X)) = h_1(X) - h_2(X)$ iff β is a root of $h_1(X) - h_2(X)$ iff $h_1(\beta) = h_2(\beta)$. This shows that Θ is both well defined and one-to-one. The rest of the proof is straightforward.

The next theorem states a simple fact which is of vast significance, as we shall later see.

(10.10) Theorem: Let F, K, and L be fields, with $F \subseteq K \cap L$, and let $\Theta : K \to L$ be an F-isomorphism. Let $g(X)$ be a polynomial in $F[X]$. Suppose that $\alpha \in K$ is a root of $g(X)$. Then $\Theta(\alpha) \in L$ is also a root of $g(X)$.

Proof: Suppose that $g(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$, with the coefficients $a_i \in F$. We are given that $g(\alpha) = 0$, so that $a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0 = 0$. Applying Θ, we have

$0 = \Theta(0) = \Theta(a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0) =$

$\Theta(a_n)\Theta(\alpha)^n + \Theta(a_{n-1})\Theta(\alpha)^{n-1} + \ldots + \Theta(a_0) =$

$a_n \Theta(\alpha)^n + a_{n-1}\ \Theta(\alpha)^{n-1} + \ldots + a_0$.

This shows that $\Theta(\alpha)$ is a root of $g(X)$, as desired.

(10.11) Corollary: Let F, K, and L be fields, with $F \subseteq K \cap L$, and let $\Theta : K \to L$ be an F-isomorphism. Suppose that $g(X) \in F[X]$. Furthermore, let $\alpha_1, \ldots, \alpha_k$ be all of the (distinct) roots of $g(X)$, and suppose that $\alpha_1, \ldots, \alpha_k$ are all in K. Then the list $\Theta(\alpha_1), \ldots, \Theta(\alpha_k)$ is a permutation of the list $\alpha_1, \ldots, \alpha_k$.

Proof: By Theorem (10.10), $\Theta(\alpha_1), \ldots, \Theta(\alpha_k)$ are roots of $g(X)$. Since $\alpha_1, \ldots, \alpha_k$ are distinct, and since Θ is one-to-one, $\Theta(\alpha_1), \ldots, \Theta(\alpha_k)$ are all distinct. Thus, $\Theta(\alpha_1), \ldots, \Theta(\alpha_k)$ are k different roots of $g(X)$. However, we are supposing that $g(X)$ only has k (distinct) roots. It follows that $\Theta(\alpha_1), \ldots, \Theta(\alpha_k)$ is the entire list of roots of $g(X)$. However, $\alpha_1, \ldots, \alpha_k$ is also the entire list of roots of $g(X)$. Thus, these two lists are the same, except perhaps for order. This shows that $\Theta(\alpha_1), \ldots, \Theta(\alpha_k)$ is a permutation of $\alpha_1, \ldots, \alpha_k$.

11. Splitting Fields

Definition: If $f(X) \in F[X]$, and if $\alpha_1, \ldots, \alpha_n$ are all of the roots of $f(X)$ in $\mathbf{C}$, then $F[\alpha_1, \ldots, \alpha_n]$ is called the splitting field of $f(X)$ over F.

Example: Since the two roots of $X^2 + 1$ are i and $-i$, the splitting field of $X^2 + 1$ over $\mathbf{Q}$ is $\mathbf{Q}[i, -i]$. However, since $-i \in \mathbf{Q}[i]$, we easily see that $\mathbf{Q}[i, -i] = \mathbf{Q}[i]$. In this example, the splitting field is generated by the single root i.

Example: Let $f(X) = X^k - 1 \in \mathbf{Q}[X]$. Let ω be a primitive k-th root of unity. Then $\omega^0 = 1, \omega^1 = \omega, \omega^2, \ldots, \omega^{n-1}$ are all of the roots of $X^k - 1$. Therefore, the splitting field of $X^k - 1$ over $\mathbf{Q}$ is $\mathbf{Q}[1, \omega, \omega^2, \ldots, \omega^{n-1}]$. However, Since every root of $X^k - 1$ is just a power of ω, we see that $\mathbf{Q}[1, \omega, \omega^2, \ldots, \omega^{n-1}] = \mathbf{Q}[\omega]$, and so in this case, the splitting field is generated by the single root ω.

In the previous two examples, the splitting field of $f(X)$ over $\mathbf{Q}$ was generated over $\mathbf{Q}$ by a single root of $f(X)$. This is not always the case, as the next example shows.

Example: Consider $X^3 - 2 \in \mathbf{Q}[X]$. Let $\alpha = \sqrt[3]{2}$ be the real cube root of 2. Also, let $\omega = -\frac{1}{2} + (\frac{\sqrt{3}}{2})i$, which we recognize as a primitive cube root of unity. Since $\omega^3 = 1$, we see that the three roots of $X^3 - 2$ are α, $\alpha\omega$, and $\alpha\omega^2$. If K is the splitting field of $X^3 - 2$ over $\mathbf{Q}$, then $K = \mathbf{Q}[\alpha, \alpha\omega, \alpha\omega^2]$. We will now show that K does not equal any of $\mathbf{Q}[\alpha]$, $\mathbf{Q}[\alpha\omega]$, or $\mathbf{Q}[\alpha\omega^2]$. Since α is a real number, clearly $\mathbf{Q}[\alpha] \subseteq \mathbf{R}$. Since $\alpha\omega$ is not a real number, and $\alpha\omega \in K$, clearly $K \not\subseteq \mathbf{R}$. Thus $K \neq \mathbf{Q}[\alpha]$. Suppose now that $K = \mathbf{Q}[\alpha\omega]$. (We will derive a contradiction.) Since $X^3 - 2$ is irreducible in $\mathbf{Q}[X]$, and α and $\alpha\omega$ are both roots of this polynomial, Theorem (10.6) shows that there is a $\mathbf{Q}$-isomorphism $\Theta : \mathbf{Q}[\alpha\omega] \to \mathbf{Q}[\alpha]$. Since we are supposing that $K = \mathbf{Q}[\alpha\omega]$, we have α, $\alpha\omega$, and $\alpha\omega^2$ all in $\mathbf{Q}[\alpha\omega]$. Thus $\Theta(\alpha)$, $\Theta(\alpha\omega)$, and $\Theta(\alpha\omega^2)$ must all be in $\mathbf{Q}[\alpha]$. Since α, $\alpha\omega$, and $\alpha\omega^2$ are all the roots of $X^3 - 2 \in \mathbf{Q}[X]$, Corollary (10.11) shows that the list $\Theta(\alpha)$, $\Theta(\alpha\omega)$, $\Theta(\alpha\omega^2)$ is just a permutation of the list α, $\alpha\omega$, $\alpha\omega^2$. Therefore α, $\alpha\omega$, and $\alpha\omega^2$ are all in $\mathbf{Q}[\alpha]$. However, this is impossible, since $\mathbf{Q}[\alpha] \subseteq \mathbf{R}$ and $\alpha\omega \notin \mathbf{R}$. This contradiction shows that $K \neq \mathbf{Q}[\alpha\omega]$. The proof that $K \neq \mathbf{Q}[\alpha\omega^2]$ is similar.

Continuing with this example, we note that $\omega = \frac{\alpha\omega}{\alpha} \in \mathbf{Q}[\alpha, \alpha\omega]$. Thus α, $\alpha\omega$, and $\alpha\omega^2$ are all in $\mathbf{Q}[\alpha, \alpha\omega]$. Therefore, $K = \mathbf{Q}[\alpha, \alpha\omega, \alpha\omega^2] \subseteq \mathbf{Q}[\alpha, \alpha\omega] \subseteq \mathbf{Q}[\alpha, \alpha\omega, \alpha\omega^2] = K$, so that we see $K = \mathbf{Q}[\alpha, \alpha\omega]$. The reader may also verify that $K = \mathbf{Q}[\alpha, \alpha\omega^2] = \mathbf{Q}[\alpha\omega, \alpha\omega^2] = \mathbf{Q}[\alpha, \omega]$.

(11.1) Exercises: a) Give an efficient description of the splitting field of $X^4 - 1$ over $\mathbf{Q}$.

b) Let $\alpha = \sqrt[4]{2}$. Note that the four roots of $X^4 - 2$ are α, $-\alpha$, αi, and $-\alpha i$. Show no one of these alone generates the splitting field of this polynomial over $\mathbf{Q}$. Show that that splitting field does equal $\mathbf{Q}[\alpha, \alpha i] = \mathbf{Q}[\alpha, i]$.

12. Galois extensions

We will be particularly interested in extensions $F \subseteq K$, when K is the splitting field of some polynomial f(X) over F. We honor Galois by naming those extensions after him.

Definition: K/F is a Galois extension if K is the splitting field of some polynomial $f(X) \in F[X]$ over F.

Remark: Recall that we are dealing with special sorts of fields, those which are subsets of $\mathbf{C}$, (i.e., number fields). In a more general setting, the term Galois extension has a different meaning than we are using here. In that more general setting, what we are calling a Galois extension is often called a normal extension. However, for number fields, normal extensions and Galois extensions turn out to be identical concepts. Thus, our terminology is correct in our setting.

(12.1) Exercises: Let $F \subseteq K \subseteq L$ be fields, with L/F Galois.

a) Show that L/K is Galois.

b) Show that K/F need not be Galois.

(12.2) Theorem: Let F, E, L, and K all be fields with $F \subseteq E, L \subseteq K$, and with K/F Galois. Suppose $\varphi : E \to L$ be an F-isomorphism. Then there is an F-automorphism Φ of K such that $\Phi|E = \varphi$. (The notation $F \subseteq E, L \subseteq K$ is shorthand for $F \subseteq E \subseteq K$ and $F \subseteq L \subseteq K$.)

Proof: Suppose that $K = F[\alpha_1, ..., \alpha_n]$ with $\alpha_1, ..., \alpha_n$ the roots of $f(X) \in F[X]$. Without loss, assume that $\alpha_1, ..., \alpha_i$ are not in E, while $\alpha_{i+1}, ..., \alpha_n$ are in E. We will induct on i. If $i = 0$, then all the α are in E, so that $E = K$. Now $\varphi(\alpha_1), ..., \varphi(\alpha_n)$ are all in $\varphi(K) = \varphi(E) = L$, so L contains $F[\varphi(\alpha_1), ..., \varphi(\alpha_n)]$. However, Corollary (10.11) shows that φ simply permutes the roots of f(X), and so $F[\varphi(\alpha_1), ..., \varphi(\alpha_n)] = F[\alpha_1, ..., \alpha_n] = K$. Thus $L = K$, and so φ is already an F-automorphism of K, so that in this case, we take $\Phi = \varphi$.

Suppose now that $i \geq 0$. In E[X], suppose the irreducible decomposition of f(X) is $f(X) = g_1(X) ... g_m(X)$. Thus, in L[X], the irreducible decomposition of f(X) is $f(X) = \varphi(g_1(X)) ... \varphi(g_m(X))$. Without loss, we may assume that α_i is a root of $g_1(X)$. Also, let β be a root of $\varphi(g_1(X))$. Note $\beta \in \{\alpha_1, ..., \alpha_n\}$, and so $\beta \in K$. By Theorem (10.9), there is an isomorphism $\Theta : E[\alpha_i] \to L[\beta]$, with $\Theta|E = \varphi$. Since $\alpha_i, \alpha_{i+1}, ..., \alpha_n$ are in $E[\alpha_i]$, induction gives the desired result.

(12.3) Corollary: Let K/F be Galois. Let g(X) be irreducible in F[X], and suppose that α and β are both roots of g(X) and are both in K. Then there is an F-automorphism Θ of K with $\Theta(\alpha) = \beta$.

Proof: By Theorem (10.6), there is an F-isomorphism $\phi : F[\alpha] \to F[\beta]$ such that $\phi(\alpha) = \beta$. Now by Theorem (12.2), there is an F-automorphism Θ of K with $\Theta|F[\alpha] = \phi$. In particular, $\Theta(\alpha) = \phi(\alpha) = \beta$.

(12.4) Theorem: Let $F \subseteq E \subseteq L$, with E/F Galois. Let ϕ be an F-automorphism of L. Then $\phi|E$ is an F-automorphism of E.

Proof: Clearly it will suffice to show that $\phi(E) = E$. Suppose that $E = F[\alpha_1, \ldots, \alpha_n]$ with $\alpha_1, \ldots, \alpha_n$ the roots of $f(X) \in F[X]$. As ϕ fixes F, we have $\phi(E) = F[\phi(\alpha_1), \ldots, \phi(\alpha_n)]$. By Corollary (10.11), ϕ simply permutes the roots of f(X). Thus $\phi(E) = F[\alpha_1, \ldots, \alpha_n] = E$.

13. Root towers

We earlier defined what it meant to say a number was obtainable by radicals over $\mathbb{Q}$, and a polynomial was solvable by radicals over $\mathbb{Q}$. We now extend those definitions to any field F, by simply replacing references to $\mathbb{Q}$ by references to F.

Definition: Let F be a field, and let $\alpha \in \mathbb{C}$. We say that α is obtainable by radicals over F if there is a finite list of numbers $c_1, c_2, c_3, \ldots, c_m = \alpha$ such that every number in this list is either in F, or is the sum, difference, product or quotient of two earlier numbers in the list, or is an k-th root, for some positive integer k, of an earlier number in the list, and such that $c_m = \alpha$.

Definition: Let $f(X) \in F[X]$. We say that f(X) is solvable by radicals over F if every root of f(X) is obtainable by radicals over F.

In this section, we will give an equivalent way of saying that f(X) is solvable by radicals over F. We need to introduce the easy concept of a root tower (not to be confused with a root cellar).

Definition: Let $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$ be fields. This sequence is called a root tower if for each $1 \leq i \leq n$, $F_i = F_{i-1}[\alpha_i]$, where α_i is an element of F_i such that ${\alpha_i}^{k_i} \in F_{i-1}$ for some positive integer k_i.

Example: $Q \subseteq Q[\sqrt{3}] \subseteq Q[\sqrt{3}][\sqrt{-1}] \subseteq Q[\sqrt{3}][\sqrt{-1}][\sqrt[3]{-2+2\sqrt{-1}}]$ is a root tower, since $(\sqrt{3})^2 \in Q$, $(\sqrt{-1})^2 \in Q[\sqrt{3}]$, and $(\sqrt[3]{-2+2\sqrt{-1}})^3 \in Q[\sqrt{3}][\sqrt{-1}]$.

Recall we saw the that roots of $X^3 - 6X + 4$ are $\alpha + \beta$, $\alpha\omega + \beta\omega^2$, and $\alpha\omega^2 + \beta\omega$, where $\alpha = \sqrt[3]{-2+2i}$, $\beta = \dfrac{2}{\sqrt[3]{-2+2i}} = \dfrac{2}{\alpha}$, and $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}\,i$.

Now $\sqrt{3} \in Q[\sqrt{3}]$, and $i \in Q[\sqrt{-1}]$, so that $\omega = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}\,i$ is in $Q[\sqrt{3}][\sqrt{-1}]$. Obviously $\alpha = \sqrt[3]{-2+2i}$ and $\beta = \dfrac{2}{\sqrt[3]{-2+2i}} = \dfrac{2}{\alpha}$ are in $Q[\sqrt[3]{-2+2i}]$. Thus, we see that the three roots of $X^3 - 6X + 4$, $\alpha + \beta$, $\alpha\omega + \beta\omega^2$, and $\alpha\omega^2 + \beta\omega$, are all in $Q[\sqrt{3}][\sqrt{-1}][\sqrt[3]{-2+2\sqrt{-1}}]$. Therefore, if K is the splitting field of $X^3 - 6X + 4$ over Q, then $K \subseteq Q[\sqrt{3}][\sqrt{-1}][\sqrt[3]{-2+2\sqrt{-1}}]$. This illustrates the truth of one direction of the next theorem.

(13.1) Theorem: Let $f(X) \in F[X]$, and let K be the splitting field of f(X) over F. Then f(X) is solvable by radicals over F if and only if there is a root tower $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n$, such that $K \subseteq F_n$.

(13.2) Exercise: Convince yourself of the truth of this theorem. (Writing out a detailed proof of this theorem is rather laborious in terms of notation, particularly the direction we did not illustrate. You may want to try to write out a detailed proof of the direction we did illustrate.)

Remark: Many people take the condition stated in this theorem to be the definition of what it means to say that f(X) is solvable by radicals over F.

14. Groups

We need to use the concept of a group. Groups are very simple mathematical structures, which are useful in a plethora of settings. This combination of simplicity and utility make groups a truly fundamental concept.

Definition: A group is a set G together with operation (which we will refer to as multiplication, unless we are in a setting in which it is more natural to call it addition) such that the following rules hold.

i) If $x,y \in G$, then $xy \in G$. (Closure)

ii) If $x,y,z \in G$ then $(xy)z = x(yz)$. (Associativity)

iii) $\exists\ 1 \in G$, $\forall x \in G$, $1x = x1 = x$. (Identity)

iv) $\forall x \in G$, $\exists\ x^{-1} \in G$, $xx^{-1} = x^{-1}x = 1$. (inverses)

Examples: a) Let $G = \mathbf{Z}$ and let the operation be addition. This is a group. Note that the identity element which satisfies rule (iii) is the integer 0, since $0 + x = x + 0 = x$, $\forall\ x \in \mathbf{Z}$. For $x \in \mathbf{Z}$, the element whose existence is dictated by rule (iv) is $-x$, since $x + (-x) = (-x) + x = 0$.

b) Let $G = \mathbf{Q}$ and let the operation be addition. This is a group.

c) Let $G = \{x \in \mathbf{Q} \mid x \neq 0\}$ and let the operation be multiplication. This is a group. The identity element satisfying rule (iii) is the rational number 1. For $x \in \mathbf{Q}$, the element whose existence is dictated by rule (iv) is $\frac{1}{x}$. Note that if we had not deleted 0 from the set G, we would not have a group, since if $x = 0$, there would be no x^{-1} with $xx^{-1} = 1$, violating rule (iv).

Remark: Notice that we do not insist that $xy = yx$. That is, we do not insist that the operation be commutative. In all of the above examples, the operation is commutative, but you will later see groups in which the operation is not commutative.

Definition: A group whose operation is commutative is called an Abelian group, (in honor of the Norwegian mathematician Abel).

(14.1) Exercises: Which of the following are groups?

a) G = the set of even integers; the operation is addition.

b) G = the set of odd integers; the operation is addition.

c) $G = \{(a, b) \mid a,b \in \mathbf{Z}\}$; the operation is

$(a, b) + (c, d) = (a + c, b + d)$.

d) $G = \{(a, b) \mid a,b \in \mathbf{Z}$ with a and b not both zero$\}$; the operation is $(a, b)(c, d) = (ac, bd)$.

e) $G = \{(a, b) \mid a,b \in \mathbb{Z}$ with a and b not both zero$\}$; the operation is $(a, b)(c, d) = (ac - bd, ad + bc)$.

f) $G = \{\alpha \in \mathbb{C} \mid \alpha \neq 0\}$; the operation is multiplication.

(Question: Can you find a connection between parts (e) and (f)?)

h) $G = \{a, b\}$ (where here, a and b are simply two symbols); the operation is determined as follows: $aa = a$, $ab = b$, $ba = b$, $bb = a$. (in tabular form, we could express this as

	a	b
a	a	b
b	b	a

.

This is a multiplication table, just like you had to memorize in elementary school.)

(14.2) Lemma: If G is a group, then the element 1 is unique.

Proof: Suppose that 1 and 1′ are both elements in G and both satisfy rule (iii) of a group. Then $1 = (1)(1')$ (by rule (iii) applied to 1′ and $x = 1$). However, $(1)(1') = 1'$ (by rule (iii) applied to 1 and $x = 1'$). Thus $1 = (1)(1') = 1'$.

(14.3) Exercises: Let G be a group.

a) Show that if $x \in G$, then the element x^{-1} given by rule (iv) is unique.

b) Show that if $x,y, z \in G$, with $xy = xz$, then $y = z$.