

5. THE FUNDAMENTAL THEOREM OF ALGEBRA

(WHY EVERY POLYNOMIAL OVER \mathbf{C} HAS A ZERO)

§5.1. Algebraically Closed Fields

If F is any field (not necessarily a subfield of \mathbf{C}) with the property that every non-constant polynomial over F has a zero in F , then F is said to be **algebraically closed**.

Example 1: \mathbf{Q} is not algebraically closed since $x^2 - 2 \in \mathbf{Q}[x]$ and has no zeros in \mathbf{Q} .

\mathbf{R} is not algebraically closed since $x^2 + 1 \in \mathbf{R}[x]$ has no zeros in \mathbf{R} .

\mathbf{C} is algebraically closed. This is just a restatement of the Fundamental Theorem of Algebra and it is this fact that we shall prove.

In the previous chapters we worked entirely inside of \mathbf{C} . Most of what we did is valid for any field. The only slight change is that where we have a field F and an element $\alpha \notin F$ we can no longer define $F[\alpha]$ to denote the smallest subfield of \mathbf{C} which contains F and α . However whenever we use the symbol $F[\alpha]$, α will belong to some larger field H and $F[\alpha]$ will denote the smallest subfield of H containing F and α .

There's another way of extending a field. If F is any field and $p(x) \in F[x]$ is prime, the quotient ring $F[x]/p(x)F[x]$ is a field which contains an isomorphic copy of F and also a zero of $p(x)$. We may therefore regard $F[x]/p(x)F[x]$ as an extension of F . So there is no such thing as a polynomial with no zeros because we can always manufacture an extension which contains such zeros. But in extending the field we are allowing our coefficients to come from this larger field and perhaps one of these new polynomials has no zero. Perhaps we will be forever extending and coming across polynomials with no zeros.

§5.2. Fixed Fields

If G is any group of automorphisms of a field F , the fixed field of G is defined to be the set of all elements of F which are fixed by every automorphism in G , that is: $\{\alpha \in F \mid \alpha^\theta = \alpha \text{ for all } \theta \in G\}$.

We leave it to the reader to check that it is a subfield of F .

Example 2: The fixed field of $G(\mathbf{C}/\mathbf{R})$ is \mathbf{R} since $G(\mathbf{C}/\mathbf{R}) = \{1, \lambda\}$ where 1 is the identity automorphism and λ is the conjugation automorphism.

§5.3. Automorphisms as Linear Transformations

Suppose that K is a finite-dimensional extension of F . Then K is a finite-dimensional vector space over F . Every automorphism in $G(K/F)$ is automatically a linear transformation from K to K (with K viewed as a vector space over F .)

But there are certainly linear transformations from K to K (viewed as a vector space over F) which are not field automorphisms. Let $L(K/F)$ denote the set of all linear transformations from K to K (with K viewed as a vector space over F). It can itself be viewed as a vector space over K with “point-wise” addition and scalar multiplication. And as we have noted, $G(K/F)$ is a subset of $L(K/F)$.

Example 3: C is a vector space of dimension 2 over R and $\{1, i\}$ is a basis. Every linear transformation of this vector space can be represented by a 2×2 matrix. So $L(C/R)$ can be identified with the ring of all 2×2 real matrices.

There are infinitely many of these. But the only two which are field automorphisms are the identity and conjugation. The matrices of these, relative to the basis $\{1, i\}$ are: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Theorem 1: $G(K/F)$ is a linearly independent subset of $L(K/F)$ as a vector space over K .

Proof: Suppose that $\lambda_1\theta_1 + \lambda_2\theta_2 + \dots + \lambda_r\theta_r = 0$ (where each $\lambda_i \in K$ and each $\theta_i \in G(K/F)$) is a non-trivial linear relationship with the least number of terms, r . Clearly each $\lambda_i \neq 0$ and the θ_i 's are distinct and $r \geq 2$. For some $\alpha \in K$, $\alpha^{\theta_1} \neq \alpha^{\theta_r}$. Now choose any $\beta \in K$. Applying $\lambda_1\theta_1 + \lambda_2\theta_2 + \dots + \lambda_r\theta_r$ to $\alpha\beta$ and β respectively we obtain:

$$\lambda_1\alpha^{\theta_1}\beta^{\theta_1} + \lambda_2\alpha^{\theta_2}\beta^{\theta_2} + \dots + \lambda_r\alpha^{\theta_r}\beta^{\theta_r} = 0 \dots (1)$$

$$\lambda_1\beta^{\theta_1} + \lambda_2\beta^{\theta_2} + \dots + \lambda_r\beta^{\theta_r} = 0 \dots (2)$$

Multiplying (2) by α^{θ_1} and subtracting from (1) we get

$$\lambda_2(\alpha^{\theta_2} - \alpha^{\theta_1})\beta^{\theta_2} + \dots + \lambda_r(\alpha^{\theta_r} - \alpha^{\theta_1})\beta^{\theta_r} = 0.$$

Since this holds for all $\beta \in K$ we have:

$$\lambda_2(\alpha^{\theta_2} - \alpha^{\theta_1})\theta_2 + \dots + \lambda_r(\alpha^{\theta_r} - \alpha^{\theta_1})\theta_r = 0. \text{ This is non-trivial since } \lambda_r(\alpha^{\theta_1} - \alpha^{\theta_r}) \neq 0 \text{ and has fewer terms than the shortest such linear relationship which is a contradiction.}$$

So $G(K/F)$ is a linearly independent subset of $L(K/F)$ as a vector space over K . Can it perhaps be a basis? For this to happen we would need $|L(K/F):K|$, the dimension of $L(K/F)$ to equal $|G(K/F)|$, the order of the group. So what is the dimension of $L(K/F)$ over K ?

Theorem 2: $|L(K/F):K| = |K:F|$.

Proof: Let K be a degree n extension of F . Now $L(K/F)$ is a vector space over K which in turn is a vector space over F and so by Theorem 7 of chapter 1:

$$|L(K/F):F| = |L(K/F):K| \times n. \text{ But Since } L(K/F) \text{ can be identified with the } n \times n \text{ matrices over } F, |L(K/F):F| = n^2. \text{ Thus } |L(K/F):K| = n.$$

Corollary: $|G(K/F)| \leq |K:F|$.

Proof: $G(K/F)$ is a linearly independent subset of a vector space of dimension $|K:F|$.

Theorem 3: If G is a group of automorphisms of a field K and F is the fixed field of G then $|G| = |K:F|$.

Proof: Let $G = \{\theta_1, \dots, \theta_m\}$, where $m = |G|$ and let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for K over F , where $n = |K:F|$. By the above corollary we have that $m \leq n$. Suppose $m < n$.

The system of equations:

$$\sum_{i=1}^n (\alpha_i^{\theta_j^{-1}}) x_i = 0$$

is a system of m equations (one for each j) in n variables (the x_1, \dots, x_n).

Since $m < n$ the system has a non-zero solution. One of the variables, say x_1 can be chosen arbitrarily to be any element of K .

Applying the appropriate θ_j to these equations we get:

$$\sum_{i=1}^n \alpha_i (x_i^{\theta_j}) = 0 \text{ for } j = 1, \dots, m.$$

Summing over j and interchanging the order of summation we get:

$$\sum_{i=1}^n \left(\sum_{j=1}^m x_i^{\theta_j} \right) \alpha_i = 0$$

Now the α_i are linearly independent over F so if we knew that each of these coefficients was in F we could conclude that they were all zero. But are they?

For all $\varphi \in G$, $\left(\sum_{j=1}^m x_i^{\theta_j} \right)^\varphi = \sum_{j=1}^m x_i^{\theta_j \varphi} = \sum_{j=1}^m x_i^{\theta_j}$ since as θ_j runs over all the elements of

G , so does $\theta_j \varphi$. Hence each $\sum_{j=1}^m x_i^{\theta_j} \in F$, the fixed field of G . Thus they are all zero.

Since x_1 could be chosen arbitrarily to be any element of K it follows that:

$$\sum_{j=1}^m x^{\theta_j} = 0 \text{ for all } x \in K.$$

Thus $x^{\sum \theta_j} = 0$ for all $x \in K$ and so $\sum \theta_j = 0$.

Thus G is a linearly dependent subset of the linearly independent set $G(K/F)$.

(Note that we are using the same field of scalars, F , in these contradictory statements.)

Hence $m = n$.

Corollary: If G is a group of automorphisms of a field F and F is the fixed field of G then G is a basis for $L(K/F)$ over K .

Example 4: $G = \{1, \lambda\}$, where 1 is the identity automorphism and λ is the conjugation automorphism, is a group of automorphisms of \mathbf{C} . The fixed field of G is \mathbf{R} so G is a basis for $L(\mathbf{C}/\mathbf{R})$ over \mathbf{C} . This means we should be able to express every element of $L(\mathbf{C}/\mathbf{R})$ uniquely in the form $u1 + v\lambda$ for some $u, v \in \mathbf{C}$. Now a typical linear transformation $f: \mathbf{C} \rightarrow \mathbf{C}$ (as a vector space over \mathbf{R}) has the form:

$$x + iy \rightarrow (ax + by) + i(cx + dy).$$

$$\text{Now } (ax + by) + i(cx + dy) = \left(\left(\frac{a+d}{2} \right) + \left(\frac{c-b}{2} \right) i \right) (x + iy) + \left(\left(\frac{a-d}{2} \right) + \left(\frac{b+c}{2} \right) i \right) (x - iy)$$

so the linear transformation can be expressed as:

$$\left(\left(\frac{a+d}{2} \right) + \left(\frac{c-b}{2} \right) i \right) 1 + \left(\left(\frac{a-d}{2} \right) + \left(\frac{b+c}{2} \right) i \right) \lambda.$$

§5.4. Fixed Fields of Polynomial Extensions

Theorem 4: If $p(x) \in F[x]$ is prime over the field F of characteristic zero, then it has no repeated zeros.

Proof: Suppose $p(x)$ has a repeated zero, α . Then $p(x) = (x - \alpha)^2 q(x)$ for some $q(x) \in F[x]$ and so α is a zero of $p'(x)$. Now if $p(x) = a_n x^n + \dots + a_0$ where $a_n \neq 0$ and $n \geq 1$ then $p'(x) = n a_n x^{n-1} + \dots$ and since F has characteristic zero, $n a_n \neq 0$. Thus $p'(x) \neq 0$ and $\deg p'(x) = n - 1$. Thus $p(x)$ and $p'(x)$ are not coprime. Hence $p(x)$ cannot be prime. Or in other words, if it is prime it cannot have a repeated zero.

Theorem 5: If K is a polynomial extension of F where F has characteristic zero then the fixed field of $G(K/F)$ is F .

Proof: Let $K = F[f(x) = 0]$ and let L be the fixed field of $G(K/F)$. Clearly $F \leq L$. Conceivably there could be elements outside of F which are fixed whenever the elements of F are.

Suppose $F < L$ and choose $\alpha \in L$ such that $\alpha \notin F$. Let $p(x)$ be the minimum polynomial of α over F . By the remainder theorem applied to $F[\alpha]$, $p(x) = (x - \alpha)q(x)$ for some $q(x) \in F[\alpha][x]$. Let H be an extension of $L[\alpha]$ which contains a zero, say β , of $q(x)$. By Theorem 4 $\alpha \neq \beta$. Now $p(\beta) = 0$ and since $p(x)$ is prime over F , it is the minimum polynomial, over F , of β as well as α . Hence there is an isomorphism from $F[\alpha]$ to $F[\beta]$ which fixes the elements of F and takes α to β . This may be extended to an isomorphism from $F[\alpha][f(x) = 0]$ to $F[\beta][f(x) = 0]$, ie an isomorphism from K to $K[\beta]$. This isomorphism fixes the elements of F and so is a non-singular linear transformation from K to $K[\beta]$, regarding both as vector spaces over F .

They therefore have the same dimension over F . But K is a subspace of $K[\beta]$ and so $K = K[\beta]$, that is $\beta \in K$. So θ is an automorphism of K which fixes the elements of F and takes α to β . This contradicts the fact that $\alpha \in L$, the fixed field of $G(K/F)$. Hence $F = L$.

§5.5. Finite-dimensional Extensions of the Real and Complex Fields

Theorem 6: There is no proper extension of \mathbf{R} of odd dimension over \mathbf{R} .

Proof: Let $\mathbf{R} < K$ such that $|K:\mathbf{R}|$ is odd. Let $\alpha \in K$ such that $\alpha \notin \mathbf{R}$. Then $\mathbf{R}[\alpha] \leq K$ and $|K:\mathbf{R}| = |K:\mathbf{R}[\alpha]| \cdot |\mathbf{R}[\alpha]:\mathbf{R}|$ from which we see that $|\mathbf{R}[\alpha]:\mathbf{R}|$ is odd. But $|\mathbf{R}[\alpha]:\mathbf{R}|$ is equal to the degree of $p(x)$, the minimum polynomial of α over \mathbf{R} . Since $p(x)$ has odd degree it has at least one real zero, β . But then $p(x) = (x - \beta)q(x)$ for some $q(x) \in \mathbf{R}[x]$, contradicting the fact that $p(x)$ is prime over \mathbf{R} .

Theorem 7: There is no extension of \mathbf{C} of degree 2.

Proof: Let $\mathbf{C} < K$ be such that $|K:\mathbf{C}| = 2$. Let $\alpha \in K$ such that $\alpha \notin \mathbf{C}$. Then $\mathbf{C}[\alpha] = K$ and the minimum polynomial of α over \mathbf{C} has degree 2. But the zeros of a polynomial over \mathbf{C} of degree 2 are themselves in \mathbf{C} by the quadratic equation formula, so $\alpha \in \mathbf{C}$, a contradiction.

§5.6. The Proof of the Fundamental Theorem of Algebra

Theorem 8: If $f(x) \in \mathbf{C}[x]$ then $f(\alpha) = 0$ for some $\alpha \in \mathbf{C}$.

Proof: Let $f(x) \in \mathbf{C}[x]$ and let $g(x) = f(x)f^\lambda(x)$ where λ is the conjugation automorphism. Then $g(x) \in \mathbf{R}[x]$.

Let $K = \mathbf{C}[g(x) = 0]$ and let $G = G(K/\mathbf{R})$. Let $|G| = 2^r m$ where m is odd. So the order of a Sylow 2-subgroup, T , of G is 2^r . Let F be the fixed field of T . By Theorem 3 $|K:F| = 2^r$. By Theorem 5 the fixed field of G is \mathbf{R} and so by Theorem 3 $|K:\mathbf{R}| = |G| = 2^r m$. Hence $|F:\mathbf{R}| = m$. By Theorem 6, $m = 1$ and so $|K:\mathbf{R}| = |G| = 2^r$.

Since $\mathbf{C} \leq K$, $r \geq 1$ and $|K:\mathbf{C}| = 2^{r-1}$. If $r = 1$, $K = \mathbf{C}$ and so the zeros of $g(x)$, and hence those of $f(x)$, are already in \mathbf{C} . Suppose $r \geq 2$. By Theorem 5 the fixed field of $G(K/\mathbf{C})$ is \mathbf{C} and so by Theorem 3 $|G(K/\mathbf{C})| = |K:\mathbf{C}| = 2^{r-1}$. Now $G(K/\mathbf{C})$ has a subgroup M of order 2^{r-2} and if H is the fixed field of M , $|K:H| = |M| = 2^{r-2}$. Thus $|H:\mathbf{C}| = 2$ which contradicts Theorem 7.

NOTE: Despite its name, the Fundamental Theorem of Algebra is actually a theorem of Analysis because it hinges on the continuity properties of the real and complex numbers as well as on the algebraic properties. But in this proof the analysis is well hidden. Can you find it?

