6. EXTENSION FIELDS

A field E is called an *extension field* of a field F if $F \leq E$, i.e. F is a subfield of E. For example, $\mathbb{R}$ is an extension field of $\mathbb{Q}$ and $\mathbb{C}$ is an extension field of $\mathbb{R}$.

Theorem 6.1. Kronecker's Theorem *Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Proof. Since $F[x]$ is a UFD, $f(x)$ is expressed as a product of irreducible polynomials. Hence it will be enough to prove the theorem in case $f(x)$ is irreducible. Consider an irreducible polynomial $p(x)$. The ideal generated by $p(x)$ in $F[x]$ is maximal, hence the factor ring $F[x]/\angle p(x)\rangle$ is a field. We can consider F as a subfield of $F[x]/\langle p(x)\rangle$ as follows: any element of F sits in $F[x]$ as a constant polynomial. Hence we only need to show that this inclusion is injective. For any two element $a, b \in F$, if we have $\overline{a} = \overline{b}$, then $a - b \in \langle p(x)\rangle$ by the definition of cosets. This means that $a - b = p(x)q(x)$ for some $q(x) \in F[x]$. Just by considering degrees of each side, we conclude that this forces $p(x)$ to be a constant polynomial which is a contradiction. Under this identification of F as a subfield of $F[x]$, the polynomial $p(x)$ is an element of the polynomial ring $\left(F[x]/\langle p(x)\rangle\right)[x]$. We evaluate this polynomial $p(x)$ at the point $x + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$. And it simply means that $p(x + \langle p(x)\rangle) = \langle p(x)\rangle = \overline{0}$, i.e. $x + \langle p(x)\rangle$ is a zero of $p(x)$ over the field $F[x]/\langle p(x)\rangle$. This finishes the proof. $\square$

Example 6.1. $\mathbb{C} = \mathbb{R}[x]/\langle x^2 + 1\rangle$, $\mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q}/\langle x^2 - \alpha\rangle$.

Definition 6.1. Given an extension field E of a field F, an element $\alpha \in E$ is said to be *algebraic over F* if there exists a nonzero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. If α is not algebraic over F, then α is said to be *transcendental over F*. When we omit to say "over F", it means that we are in the context of the extension field $\mathbb{C}$ over the rational field $\mathbb{Q}$.

Example 6.2. π, e are transcendental elements of $\mathbb{R}$ over $\mathbb{Q}$. $\sqrt{2}, \sqrt{1+\sqrt{2}}, \sqrt{1+\sqrt{1+\sqrt{2}}}$ are algebraic elements of $\mathbb{R}$ over $\mathbb{Q}$. π is an algebraic element of $\mathbb{R}$ over $\mathbb{R}$ or $\mathbb{Q}(\pi)$.

Theorem 6.2. *Let E be an extension field of a field F and let $\alpha \in E$. Let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism of $F[x]$ into E such that $\phi_\alpha|_F = Id_F$ and $\phi_\alpha(x) = \alpha$. (This completely determines ϕ) Then α is transcendental over F if and only if ϕ_α is a one-to-one map, i.e. ϕ_α gives an isomorphism of $F[x]$ with the subdomain $\phi_\alpha(F[x])$ of E.*

Theorem 6.3. *Let E be an extension field of F, and let $\alpha \in E$ where α is algebraic over F. Then there is an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. $p(x)$ is uniquely determined up to a constant multiplication factor in F and is a polynomial of minimal degree≥ 1 in $F[x]$ having α as a zero. Any other polynomial which has α as a zero is a multiple of $p(x)$.*

Definition 6.2. Let E be an extension field of a field F, and let $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ having the property of the above theorem is called the *irreducible polynomial for* α *over* F and will be denoted by irr(α, F). The degree of the polynomial irr(α, F) is the *degree of* α *over* F, denoted by deg(α, F).

Example 6.3. irr($\sqrt{1+\sqrt{3}}, \mathbb{Q}$) = $x^4 - 2x^2 - 2$. deg($\sqrt{2}, \mathbb{Q}$)=2. deg($\sqrt{2}, \mathbb{R}$)=1.