FEBRUARY 6 NOTES

1. 13.1: Basic Theory of Field Extensions

Reminder from last time:

Theorem 1.1. *Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then, there exists a field extension K of F in which $p(x)$ has a root. We construct K as $K = F[x]/(p(x))$ and we can explicitly write the elements of K: let $\theta = \overline{x} \in K$. Then, the elements $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ are a basis for K as a vector space over F, so*

$$K = \{b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} \mid b_i \in F\}$$

consists of all polynomials of degree $< n$ in θ and K has degree n as an extension over F.

Small commentary: we can use this description to understand multiplication and inverses in K. Suppose that $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ (note that we may assume $a_n = 1$ by multiplying $p(x)$ by $(a_n)^{-1}$). Then, because θ is a root of $p(x)$, $\theta^n = -(a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0)$. So, given two elements of K, we may multiply them and replace any powers θ^n (or higher) by this expression in lower degree terms. Another way of writing this is to say, given two polynomials $f(\theta)$ and $g(\theta)$ in K, their product is $r(\theta)$, where $f(x)g(x) = r(x) \pmod{p}(x)$ and $r(x)$ is the remainder under polynomial long division by $p(x)$.

We can also understand θ^{-1} by using that $p(\theta) = 0$, i.e. $\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta = -a_0$, i.e. $\theta(\theta^{n-1} + a_{n-1}\theta^{n-2} + \cdots + a_1) = -a_0$, so we see that

$$\theta^{-1} = (-a_0)^{-1}(\theta^{n-1} + a_{n-1}\theta^{n-2} + \cdots + a_1).$$

To find inverses of general elements $q(\theta) \in K$, you need to find another polynomial $q^{-1}(\theta) \in K$ such that $qq^{-1}(\theta) = 1$; equivalently, $qq^{-1}(x)$ is equal to 1 plus some multiple of $p(x)$. This can be done using long division, the Euclidean algorithm, ...

We ended last time with a criterion for irreducibility:

Eisenstein's Criterion: let $f(x) \in \mathbb{Z}[x]$ be a polynomial, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Suppose that there is some prime number p such that $p \mid a_i$ for each $i \in \{0, \dots, n-1\}$, but $p^2 \nmid a_0$. Then, $f(x)$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Example 1.2. The polynomial $p(x) = x^3 - 2$ is irreducible over $\mathbb{Q}[x]$ by Eisenstein's criterion (with the prime equal to 2), so there is a degree three field extension

$$\mathbb{Q}[x]/(x^3 - 2) \cong \{a + b\theta + c\theta^2 \mid \theta^3 = 2, \quad a, b, c \in \mathbb{Q}\}.$$

Right now, θ is just a symbol. However, using our previous knowledge of number systems, we want to represent θ with an actual 'number' (e.g. $\theta = \sqrt[3]{2}$ in the previous example). To do this, we make the following definition:

Definition 1.3. Let K be an extension of F and let $\alpha, \beta, \dots$ be a collection of elements in K. The smallest subfield of K containing both F and the elements $\alpha, \beta, \dots$ is called the **field generated by** $\alpha, \beta, \dots,$ **over** F and denoted by $F(\alpha, \beta, \dots)$.

Note that such a smallest field exists: certainly a subfield of K containing F and these elements exists (namely, K), and the intersection of subfields is a subfield, so we could define $F(\alpha, \beta, \dots)$ to be the intersection of all subfields containing F and $\alpha, \beta, \dots$.

Definition 1.4. If $K = F(\alpha)$ is generated by a single element over F, then K is a **simple extension of** F and α is called a **primitive element** for the extension.

Theorem 1.5. *Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. If K is any extension of F containing a root α of $p(x)$, then $F(\alpha) \cong F[x]/(p(x))$.*

Proof. Let $\phi : F[x] \to F(\alpha) \subset K$ be the homomorphism $a(x) \mapsto a(\alpha)$. Since $p(\alpha) = 0$, $p(x) \in \ker \phi$, and hence there is an induced homomorphism $\phi : F[x]/(p(x)) \to F(\alpha)$. Because $F[x]/(p(x))$ is a field and this map is not zero, it must be injective and hence $F[x]/(p(x))$ is isomorphic to its image. By construction, the image is a subfield of $F(\alpha)$ containing α and F, but $F(\alpha)$ is the smallest subfield of K with this property, so the image must be all of $F(\alpha)$ and therefore ϕ is surjective and hence an isomorphism. ☐

Using this with our previous description of $F[x]/(p(x))$, we see that, in the previous theorem, $F(\alpha) \subset K$ is exactly the set

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\} \subset K.$$

Now we use this to simplify notation. For example, above we constructed

$$\mathbb{Q}[x]/(x^3 - 2) \cong \{a + b\theta + c\theta^2 \mid \theta^3 = 2, \quad a, b, c \in \mathbb{Q}\}.$$

Let $\sqrt[3]{2} \in \mathbb{R}$ denote the cube root of 2. Then, the subfield $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{R}$ is exactly

$$\mathbb{Q}[x]/(x^3 - 2) \cong \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}.$$

We finish this section with one more theorem.

Theorem 1.6. *Let $\phi : F \to F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x)$ be its image by applying the map ϕ. Let α be a root of $p(x)$ in some extension of F and β a root of $p'(x)$ in some extension of F'. Then, there is an isomorphism $\sigma : F(\alpha) \to F'(\beta)$ extending ϕ and mapping α to β.*

Proof. By definition, $F(\alpha) \cong F[x]/(p(x))$, sending α to x (similarly, $F'(\beta) \cong F'[x]/(p'(x))$). By construction, $F[x]/(p(x)) \cong F'[x]/(p'(x))$, and composing these isomorphims gives the desired result. ☐

2. 13.2: Algebraic Extensions

Definition 2.1. Let F be a field and let K be an extension of F. An element $\alpha \in K$ is **algebraic** over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F, we say that α is **transcendental** over F. The extension K/F is **algebraic** if every element of K is algebraic over F.

Remark 2.2. If α is algebraic over F, then it is algebraic over any extension L of F (because algebraicity over F implies it is a root of a polynomial in $F[x]$, and $F \subset L$, so it is a root of a polynomial in $L[x]$).

Example 2.3. We won't prove this now, but you may be familiar with the terminology already. For example, π is transcendental over $\mathbb{Q}$ because there is no polynomial with coefficients in $\mathbb{Q}$ such that π is a root of it (but these things are hard to prove!!). Numbers like $\sqrt[3]{2}$ are algebraic over $\mathbb{Q}$ because by definition, it is the root of $x^3 - 2 = 0$.

Proposition 2.4. *Let α be algebraic over F. Then, there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.*

This polynomial is called the ***minimal polynomial*** *for α over F. If F is clear from context, it is denoted simply by $m_\alpha(x)$. The* ***degree*** *of α is defined to be the degree of $m_\alpha(x)$.*

Proof. Suppose $g(x) \in F[x]$ is a polynomial of minimal degree with α as a root. We may assume that $g(x)$ is monic (by multiplying by a constant). Suppose first that $g(x)$ was reducible: then $g(x) = a(x)b(x)$ for some $a, b \in F[x]$ with $\deg a, b < \deg g$. Then, because $F \subset K$, $0 = g(\alpha) = a(\alpha)b(\alpha)$, but K is a field, so this implies that either $a(\alpha) = 0$ or $b(\alpha) = 0$, contradicting the minimality of the degree of g. Therefore, $g(x)$ is a monic irreducible polynomial with α as a root. If $f(x) \in F[x]$ is any polynomial with α as a root, then by the Euclidean Algorithm, $f(x) = q(x)g(x) + r(x)$ for some polynomials $q, r \in F[x]$ with $\deg r < \deg g$. However, this implies that $0 = f(\alpha) = q(\alpha)g(\alpha) + r(\alpha) = 0 + r(\alpha)$, so $r(\alpha) = 0$, and α is a root of $r(x)$. Because $\deg r < \deg g$, this is possible if and only if $r = 0$, so $f(x)$ is divisible by $g(x)$. This proves that $g(x)$ divides any polynomial with α as a root, and in particular divides any other monic irreducible polynomial with α as a root, so $g(x) = m_\alpha(x)$ is unique. □

Corollary 2.5. By the remark and proposition, if L/F is any field extension and α is algebraic over F, then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$.

Proposition 2.6. *Let $\alpha \in K$ be algebraic over F and let $F(\alpha)$ be the field generated by α over F. Then, $F(\alpha) \cong F[x]/(m_\alpha(x))$ and $[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha$.*

Proof. This follows directly from the second-to-last theorem in the previous section. □

Example 2.7. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$: this polynomial is monic and has 2 as a root and is irreducible by Eisenstein's criterion. Therefore, $\sqrt{2}$ has degree 2 over $\mathbb{Q}$. Similarly, for any $n > 1$, $\sqrt[n]{2}$ has minimal polynomial $x^n - 2$ over $\mathbb{Q}$.

Proposition 2.8. *If $\alpha \in K/F$ with $[K : F] = n$, then $\deg \alpha \leq n$. An element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite.*

Proof. Suppose α is an element of a finite extension K of F with $[K : F] = n$. Then, the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ must be linearly dependent, so there exist some elements $b_i \in F$ not all zero such that

$$b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0,$$

i.e. α is the root of the nonzero polynomial $b_0 + b_1x + \cdots + b_nx^n$ which has degree $\leq n$. Therefore, $\deg \alpha \leq n$. Applying this to $K = F(\alpha)$ we see that if $F(\alpha)/F$ is finite, then α is algebraic over F. Conversely, if α is algebraic over F, then $[F(\alpha) : F] = \deg m_\alpha < \infty$. □

Corollary 2.9. If K/F is finite, then it is algebraic.

Proof. By the previous proposition, for any $\alpha \in K$, $\deg \alpha \leq n$ so α is algebraic over F. □