FEBRUAY 1 NOTES

1. 13.1: Basic Theory of Field Extensions

Definition 1.1. A **field** F is a commutative ring with identity in which every nonzero element has an inverse. We denote the identity by 1_F or 1 if F is clear from context.

The **characteristic** of a field F, denoted $\mathrm{char}(F)$ is the smallest positive integer n such that $n(1_F) = 1_F + 1_F + \cdots + 1_F$ (n times) is equal to 0. If no such n exists, we define $\mathrm{char}(F) = 0$.

Observe that $(n \cdot 1_F) + (m \cdot 1_F) = (n + m) \cdot 1_F$ and $(n \cdot 1_F)(m \cdot 1_F) = (nm) \cdot 1_F$. The second statement implies that the characterstic of any field, if not zero, must be prime: if $n = ab$ is composite and $n \cdot 1_F = 0$, then $(a \cdot 1_F)(b \cdot 1_F) = 0$ and as F is an integral domain, one of these terms must be 0. Therefore, the smallest positive integer such that $n \cdot 1_F = 0$ must be prime. Also, if $\mathrm{char}(F) = p$, then $p \cdot 1_F = 0$, so for any $a \in F$, $p \cdot a = p \cdot (1_F a) = (p \cdot 1_F)a = 0$, so $a + a + \cdots + a = 0$.

Therefore, we have just proven the following:

Proposition 1.2. *For any field F, $\mathrm{char}(F)$ is either 0 or a prime p. If $\mathrm{char}(F) = p$, then for any $a \in F$, $p \cdot a = 0$.*

Example 1.3. We have $\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = 0$. The finite field $\mathbb{F}_p := \mathbb{Z}_p$ has $\mathrm{char}(\mathbb{F}_p) = p$. The field of rational functions with coefficients in $\mathbb{F}_p$ has $\mathrm{char}(\mathbb{F}_p(x)) = p$.

Defining $(-n) \cdot 1_F = -(n \cdot 1_F)$ and $0 \cdot 1_F = 0$, we have a ring homomorphism $\phi : \mathbb{Z} \to F$ for any field sending $n \mapsto n \cdot 1_F$. The kernel of this map is clearly $\ker \phi = \mathrm{char}(F)\mathbb{Z} = \langle \mathrm{char}(F) \rangle$. By the First Isomorphism Theorem, this implies that there is an injection of $\mathbb{Z}$ (if $\mathrm{char}(F) = 0$) or $\mathbb{Z}/p\mathbb{Z}$ (if $\mathrm{char}(F) = p$) into F. Since F is a field, it must contain the field of fractions of this subring, i.e. F contains $\mathbb{Q}$ if $\mathrm{char}(F) = 0$, and F contains $\mathbb{F}_p$ if $\mathrm{char}(F) = p$. By construction, this is the smallest subfield of F containing 1_F.

Definition 1.4. The **prime subfield** of a field F is the smallest subfield of F containing 1_F (sometimes referred to as the *subfield generated by* 1_F). It is isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$.

Example 1.5. The prime subfield of $\mathbb{Q}$ and $\mathbb{R}$ is $\mathbb{Q}$. The prime subfield of $\mathbb{F}_p(x)$ is $\mathbb{F}_p$.

Definition 1.6. If K is a field containing a subfield F, then K is an **extension of** F, denoted K/F (read 'K over F'). Every field is an extension of its prime subfield.

Note that, if K is an extension of F, then K is naturally an F-module by multiplication in K. Modules over fields are *the same* as vector spaces over fields, so any field extension K of F is a vector space over F.

Definition 1.7. The **degree** (or **index**) of a field extension K/F is $[K : F] = \dim_F K$, the dimension of the vector space K over F. K is said to be a **finite** extension of F if $[K : F]$ is finite and **infinite** otherwise.

Example 1.8. $\mathbb{C}$ contains $\mathbb{R}$, so $\mathbb{C}$ is an extension of $\mathbb{R}$. By construction, $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$ with basis $\{1, i\}$ (i.e. every element in $\mathbb{C}$ can be written as $a \cdot 1 + b \cdot i$ for $a, b \in \mathbb{R}$), so $[\mathbb{C} : \mathbb{R}] = 2$.

We could consider the previous example in 'reverse': there is a polynomial over $\mathbb{R}$, namely $x^2 + 1 = 0$, that has no solution in $\mathbb{R}$, and $\mathbb{C}$ is an extension of $\mathbb{R}$ in which the polynomial $x^2 + 1$ has a root. This type of extension will be the focus of the first part of this chapter. Namely: if $p(x) \in F[x]$, does there exist an extension K of F containing a root of $p(x)$? containing all roots of $p(x)$? is the extension unique? etc!

Theorem 1.9. *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.*

Proof. Define $K = F[x]/(p(x))$, and recall that, if F is a field, $F[x]$ is a Euclidean domain (via polynomial long division) and hence a PID. Therefore, because $p(x)$ is irreducible (and hence prime) so $(p(x))$ is maximal. Therefore, $K = F[x]/(p(x))$ is a field. Via the canonical projection map $F[x] \to F[x]/(p(x))$ restricted to F, there is a homomorphism $\phi : F \to K$. This sends $1_F \to 1_K$ by construction, which implies that $\phi : F \to \phi(F)$ is an isomorphism (exercise: if $\phi : F \to K$ is any field homomorphism, it is either identically 0 or injective). Therefore, $F \cong \phi(F) \subset K$ so K is an extension of F. Furthermore, let $\overline{x}$ be the image of x in the quotient $K = F[x]/(p(x))$. We have $p(\overline{x}) = \overline{p(x)} = p(x) \pmod{p}(x) = 0$, so $p(\overline{x}) = 0$ and $\overline{x} \in K$, so therefore p has a root in K. □

We can actually write the elements of K very explicitly:

Theorem 1.10. *Let $p(x) \in F[x]$ be an irreducible polynomial of degree n and let $K = F[x]/(p(x))$. Let $\theta = \overline{x} \in K$. Then, the elements $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ are a basis for K as a vector space over F, so*

$$K = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid a_i \in F\}$$

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

Proof. Let $a(x)$ be any polynomial in $F[x]$. Then, by polynomial long division, we can write

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

where $\deg r(x) < n$, and $a(x) = r(x) \pmod{p}(x)$, every coset (or 'residue class') in the quotient field $F[x]/(p(x))$ has a representative of degree $< n$. Therefore, $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ spans K as a vector space over F, so we just need to verify their linear independence. Consider a linear combination

$$b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0$$

where $b_i \in F$. This implies that $b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} = 0 \pmod{p}(x)$, i.e. $b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$ is divisible by $p(x)$. Because $\deg p(x) = n$, this is possible if and only if $b_i = 0$ for all i, i.e. the only linear combination

$$b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0$$

is trivial. Therefore, $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is linearly independent and hence a basis for K. □

From here, we can also explicitly understand addition and multiplication in K. Addition is defined component-wise, and to multiply, suppose that $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ (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 easily 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

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

In general, finding inverses can be done using the Euclidean algorithm.

Example 1.11. If $F = \mathbb{R}$ and $p(x) = x^2 + 1$, we obtain $K = \mathbb{R}[x]/(x^2 + 1)$ an extension of degree 2. Exercise: show that, for $a + b\theta$ and $c + d\theta$ in K, $(a + b\theta)(c + d\theta) = (ac - bd) + (ad + bc)\theta$.

We can identify this field with $\mathbb{C}$: from the exercise, the map

$$\phi : \mathbb{R}[x]/(x^2 + 1) \to \mathbb{C}$$

given by $\phi(a + bx) = a + bi$ is a homomorphism, and it is clearly bijective, hence an isomorphism.

We could do the same construction with $F = \mathbb{Q}$, and get a field which we denote $\mathbb{Q}(i)$. This is a degree 2 extension of $\mathbb{Q}$ containing i, and a subfield of $\mathbb{C}$ (but not all of $\mathbb{C}$!).

This construction only applies for *irreducible* polynomials. Recall (or discover?) the following test for irreducibility of polynomials over $\mathbb{Q}$ (see Chapter 9.4, Corollary 14):
Eisenstein's Criterion: let $f(x) \in \mathbb{Z}[x]$ be a polynomial, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. 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 1.12. 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

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