Lecture 16: Basics For Field Extensions

We now turn our attention to study fields. If 1_F is the multiplicative identity of the field F then $A = \{ n \cdot 1_F \mid n \in \mathbb{Z} \}$ is an additive subgroup of F where $2 \cdot 1_F = 1_F + 1_F$ or $-2 \cdot 1_F = -1_F + (-1_F)$ etc. Then either A is infinite or $\exists\, n \in \mathbb{N}$ for which $n \cdot 1_F = 0$, the smallest such $n \in \mathbb{N}$ is the characteristic of F. I believe you saw in Math 421 that, for a ring, which F is,

$$n \cdot 1_F + m \cdot 1_F = (n+m) \cdot 1_F$$

$$(n \cdot 1_F)(m \cdot 1_F) = mn \cdot 1_F$$

We defined before, but I include here for completeness

Def^n/ The characteristic of a field is defined to be smallest integer $p \in \mathbb{N}$ such that $p \cdot 1_F = 0$ if such p exists ($ch(F) = p$) and otherwise we say F has $ch(F) = 0$.

This brings us to the 1st proposition in D&F §13.1

Proposition: The characteristic of a field F, $ch(F)$ is either 0 or a prime p. If $ch(F) = p$ and $\alpha \in F$ then

$$p \cdot \alpha = \underbrace{\alpha + \alpha + \cdots + \alpha}_{p\text{-times}} = 0$$

As we discussed $\varphi: \mathbb{Z} \longrightarrow F$ given by $\varphi(n) = n \cdot 1_F$ defines a ring homomorphism where either $\ker\varphi = \{0\}$ for $ch(F) = 0$ or $\ker\varphi = p\mathbb{Z}$ for $ch(F) = p$. Hence,

$$\bar{\varphi}: \mathbb{Z}/\ker\varphi \longrightarrow F$$

gives an injection of $\mathbb{Z}$ or $\mathbb{Z}_p$ into F in $\varphi(\mathbb{Z})$ then since F is a field we see the field of fractions generated by $\varphi(\mathbb{Z})$ gives a subfield of F isomorphic to either $\mathbb{Q}$ $(ch(F)=0)$ or $\mathbb{Z}_p$ $(ch(F)=p)$ $\underbrace{\mathbb{Z}_p = \mathbb{F}_p}$ Dummit & Foote.

Def'n The <u>prime subfield</u> of a field F is the subfield generated by the multiplicative identity 1_F of F. (it's either $\mathbb{Q}$ or $\mathbb{F}_p$)

We usually use $1_F = 1$ in what follows, but keep in mind that $2 = 1+1$ means $2 \cdot 1_F = 1_F + 1_F$ etc.

E1 $\mathbb{Q}$ is prime subfield of $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Q}$.

E2 $\mathbb{F}_p$ is prime subfield of $\mathbb{F}_p$ or $\mathbb{F}_p(t)$
↳ up to <u>isomorphism</u>, we identify constant polynomials in $\mathbb{F}_p(t)$ with $\mathbb{F}_p$

E3 $\mathbb{R}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{R}[x],\ g(x) \neq 0 \right\}$
has prime subfield isomorphic to $\mathbb{Q}$, so we just say it is $\mathbb{Q}$.

Def^n/ If K is a field containing the subfield F, then K is said to be an extension field of F, denoted K/F.

We write

K
|
F ← base field of the extension

For example, every field is an extension of itself and of its prime subfield. Notice we can multiply elements of K by scalars in F thus K is a <u>vector space</u> over F.

Def^n/ The <u>degree</u> of a field extension K/F is defined by $[K:F] = \dim_F K$. If $[K:F] < \infty$ then the extension is said to be <u>finite</u>

Recall that if $\varphi: F \longrightarrow F'$ is a homomorphism of fields then since $\ker\varphi$ is an ideal of F it must be either 0 or F hence $\varphi = 0$ or φ is an injection. The take-away we should keep in mind,

<u>Proposition</u>: any nonvanishing field homomorphism is necessarily an injection.

Thm (3) (Kronecker's)

Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then $\exists$ a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy shows $\exists$ an extension of F in which $p(x)$ has a root.

Proof: construct $K = F[x]/(p(x))$ and note K is a field since $p(x)$ irred. in $F[x] \Rightarrow (p(x))$ maximal hence $F[x]/(p(x))$ is a field. Furthermore,

$\pi : F[x] \longrightarrow K$ by $\pi(f(x)) = f(x) + (p(x))$

gives homomorphism whose restriction $\pi|_F : F \to K$ naturally injects $\pi|_F(F) \subseteq K$ as $\pi|_F \not\equiv 0$. Thus $F \cong \pi_F(F) \subseteq K$. It remains to show $p(x)$ has root in K. Let $\alpha = x + (p(x))$ then if $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ then we have

$$\begin{aligned} p(\alpha) &= a_0 + a_1\alpha + \cdots + a_n\alpha^n \\ &= a_0 + a_1 x + \cdots + a_n x^n + (p(x)) \\ &= (p(x)) \\ &= 0 \quad (\text{in } K) \end{aligned}$$

Thus $p(\alpha) = 0$ for $\alpha \in K$. //

Remark: if you like D&F's argument on p. 513 better, go for it.

Th^{m}(4) Let $P(x) \in F[x]$ be irred. with $\deg(P(x)) = n$ and let $K = F[x]/_{(P(x))}$. Let $\theta = x + (P(x)) \in K$. Then the elements

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

are basis over F for K and so $[K:F] = n$.

Hence, $K = \{ a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, \ldots, a_{n-1} \in F \}$

Proof: my proof of Th^{m}(3) with $\alpha = \theta$ shows that $\text{span}_F\{1, \theta, \theta^2, \ldots, \theta^{n-1}\} = K$, but to be more careful we can use division algorithm for any $a(x) \in F[x]$ we divide by $P(x)$ to obtain $q(x)$, $r(x)$ such that

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

where $r(x) = 0$ or $\deg(r(x)) < n$. Thus,

$$a(\theta) = q(\theta)P(\theta) + r(\theta) = r(\theta) \quad (P(\theta) = 0 \text{ in } K)$$

Then $r(\theta) = r_0 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}$ hence $\{1, \theta, \ldots, \theta^{n-1}\} = S$ is spanning set for K. It remains to show S LI.

Towards $\rightarrow\leftarrow$ suppose $\exists\, b_0, \ldots, b_{n-1} \in F$, not all zero, such that $b_0 \cdot 1 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0$. Then

$b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in (P(x))$ $\therefore$ $b(x)$ is divided by $P(x)$ which is impossible since $\deg(b(x)) \leq n-1$ and $\deg(P(x)) = n$. //

Corollary (5)

Let K be as in Th^{n}(4) and let $a(\theta), b(\theta) \in K$ be two polynomials of deg. less than n in θ. Then addition in K is defined by usual poly. addition and multiplication in K is defined by

$$a(\theta)\, b(\theta) = r(\theta)$$

where $r(x)$ is remainder obtained from dividing $a(x)\, b(x)$ by $p(x)$ in $F[x]$.

If F is a subfield of K and $\alpha \in K$ then the collection of subfields containing both F and α is nonempty (take K for instance.). Then since intersection of subfields is once more a subfield we can focus our attention on the intersection of <u>all</u> subfields containing F and α, hence we define:

Def^{n}/ Let K be extension of F and let $\alpha, \beta, \ldots$ be elements of K. Then the <u>smallest</u> subfield of K containing both F and the elements $\alpha, \beta, \ldots$ is denoted $F(\alpha, \beta, \ldots)$ and this field is called the field <u>generated</u> by $\alpha, \beta, \ldots$

If $K = F(\alpha)$ then K is <u>simple</u> extension

Th^{n} (6)

Let F be a field and $P(x) \in F[x]$ an irreducible polynomial. Suppose K is an extension field of F containing a root α of $P(x)$; $P(\alpha) = 0$. Let $F(\alpha)$ denote subfield generated by F and α. Then $F(\alpha) \cong F[x]/(P(x))$.

Proof: pg. 517 of D&F, § 13.1. Very nice.

Suppose K is an extension field containing α a root of the irreducible polynomial $P(x) \in F[x]$. Consider the natural homomorphism

$$\varphi : F[x] \longrightarrow F(\alpha) \subseteq K$$

given by $\varphi(a(x)) = a(\alpha)$. Then as $P(\alpha) = 0$ is given we find $P(x) \in \ker \varphi$ thus (abusing notation slightly)

$$\varphi : F[x]/(P(x)) \longrightarrow F(\alpha)$$

is well-defined (this is an "induced homomorphism) and as $(P(x))$ is maximal ideal we find $\operatorname{im}(\varphi) \subseteq F(\alpha)$ is a field which contains both F and α ($\varphi(x) = \alpha$, $\varphi(c) = c$ $\forall c \in F$) thus $\operatorname{im}\varphi = F(\alpha)$ as $F(\alpha)$ is smallest field containing both F & α. Thus,

$$F(\alpha) \cong F[x]/(P(x))$$

Corollary (7): If $P(x)$ is irred. with $\deg(P(x)) = n$ and $P(x) \in F[x]$ where K/F contains $\alpha \in K$ s.t. $P(\alpha) = 0$ then

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\} \subseteq K$$

The importance of Th^{n} 6 is it shows all the roots of an irreducible polynomial share the same role in extending the base field. There's a symmetry among the roots.

E4 Consider $P(x) = x^2 - 2 \in \mathbb{Q}[x]$ then $\alpha = \pm\sqrt{2} \in \mathbb{R}$ and $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2}) \cong \dfrac{\mathbb{Q}[x]}{(x^2-2)}$ we might notice $\varphi(a+b\sqrt{2}) = a - b\sqrt{2}$ gives the isomorphism from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(-\sqrt{2})$. In fact, it's an automorphism since $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$.

E5 Consider $P(x) = x^3 - 2 \in \mathbb{Q}[x]$ is irred. by Eisenstein, $p = 2$. Furthermore $z^3 = 2$ has solutions $z = \sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$ where $\omega = \exp\left(\frac{2\pi i}{3}\right) = \frac{-1+i\sqrt{3}}{2}$ and $\omega^2 = \frac{-1-i\sqrt{3}}{2}$ which you could derive via completing the square,

$$\begin{aligned} x^3 - 2 &= \left(x - \sqrt[3]{2}\right)\left[x^2 + \sqrt[3]{2}x + \left(\sqrt[3]{2}\right)^2\right] \\ &= \left(x - \sqrt[3]{2}\right)\left(\left(x + \frac{\sqrt[3]{2}}{2}\right)^2 - \left(\frac{\sqrt[3]{2}}{2}\right)^2 + \left(\sqrt[3]{2}\right)^2\right) \\ &= \left(x - \sqrt[3]{2}\right)\left(\left[x + \frac{\sqrt[3]{2}}{2}\right]^2 + \left(\sqrt[3]{2}\right)^2\left(1 - \frac{1}{4}\right)\right) \\ &= \left(x - \sqrt[3]{2}\right)\left(x + \sqrt[3]{2}\left(\frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\right)\left(x + \sqrt[3]{2}\left(\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\right) \end{aligned}$$

Anyway, cumbersome calculations aside,

$$\mathbb{Q}\left(\sqrt[3]{3}\right) \cong \frac{\mathbb{Q}[x]}{(x^3-2)} \cong \mathbb{Q}\left(\omega\sqrt[3]{3}\right) \cong \mathbb{Q}\left(\omega^2\sqrt[3]{3}\right)$$

Th$^{\text{m}}$(8) Let $\varphi : F \longrightarrow F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be irred. and $p'(x) \in F'[x]$ be the irred. polynomial obtained by applying φ to the coeff. of $p(x)$. Let α be a root of $p(x)$ in some extension of F and let β be the root of $p'(x)$ in some extension of F'. Then $\exists$ an isomorphism

$$\sigma : F(\alpha) \longrightarrow F'(\beta)$$

generated by mapping $\alpha \longmapsto \beta$ and extending φ in the sense $\sigma|_F = \varphi$.

Proof: Given $\varphi : F \longrightarrow F'$ an isomorphism of fields. We can show $(p(x))$ maps to $(p'(x))$ under the induced ring homomorphism $\widetilde{\varphi} : F[x] \longrightarrow F'[x]$ given by mapping coefficients under φ. It follows $(p'(x))$ is maximal

$$F(\alpha) \cong \frac{F[x]}{(p(x))} \cong \frac{F'[x]}{(p'(x))} \cong F'(\beta)$$

Then if $\alpha \longmapsto x \longmapsto x' \longmapsto \beta$ defines σ this gives the Th$^{\text{m}}$. (composition of isomorphisms is isomorphism). //

Th$^{\text{m}}$(8)

$$\begin{array}{ccc} \sigma : F(\alpha) & \xrightarrow{\ \sim\ } & F'(\beta) \\ \Big| & & \Big| \\ \varphi : F & \xrightarrow{\ \sim\ } & F' \end{array}$$

Remark: I believe $\varphi : F \xrightarrow{\sim} F'$ indicates φ is an *isomorphism* from F to F'.