NAP 2018, NOTES ON CLASS #7, 17 MAY, 2018

• We finished the proof of
Proposition 1.27$\frac{1}{4}$: Let α be an element of an extension field K of F, with α algebraic over F. Let I be the kernel of the "evaluation" homomorphism
$\psi_\alpha : F[X] \to F[\alpha]$ by $\psi_\alpha(g(X)) = g(\alpha)$. Let $p(X)$ be a monic polynomial in $F[X]$. These conditions on $p(X) \in F[X]$ are equivalent:

(a) $p(\alpha) = 0$ and $p(X)$ has least degree among all *non-zero* polynomials $f(X) \in F[X]$ such that $f(\alpha) = 0$.
(b) $I = p(X)F[X] = (p(X)\,)$, that is, $p(X)$ generates the ideal I.
(c) $p(\alpha) = 0$ and $p(X)$ is irreducible.

• **Remark1.27$\frac{1}{3}$:** Let α be an element of an extension field K of F such that $f(\alpha) = 0$, for some non-zero $f(X) \in F[X]$. Then:
(1) $[F(\alpha) : F] \leq$degee $f(X)$.
(2) $[F(\alpha) : F] \leq [K : F]$. Note that $[K : F]$ might be ∞.

• **Theorem 1.27$\frac{3}{4}$:** Let α be an element of a extension field K of F. These conditions are equivalent:
(1) α is algebraic.
(2) $F[\alpha] = F(\alpha)$.
(3) $F[\alpha]$ is finite-dimensional as a vector space over F.

• The next theorem is related to what the book calls "Stem fields". Given any non-constant polynomial $g(X) \in F[X]$, where F is any field, we can always find an extension field of F in which $g(X)$ has a root. First choose an irreducible factor of $g(X)$; if we can find a root of this irreducible factor, we'll have a root of $g(X)$.
Theorem 1.25: Construction of extension fields with roots. Let F be a field and $p(X) \in F[X]$ a monic irreducible polynomial of degree m. Let $I = (p(X)) = p(X)F(X)$, the ideal of $F[X]$ generated by $p(X)$. Then:
(1) $F[x] = \frac{F[X]}{(p(X))}$, where x is the coset $X + I$, is an extension field of degree m over F, and $p(x) = 0$.
(2) If K/F is a field extension, and $\alpha \in K$ satisfies $p(\alpha) = 0$, then there exists a field isomorphism $\varphi = \varphi_\alpha : F[x] \overset{\cong}{\to} F[\alpha]$ such that $\varphi(x) = \alpha$ and $\varphi(c) = c$ for each $c \in F$. Note that $\varphi((f(x))) = f(\alpha)$ for each $f(X) \in F[X]$.

$$\begin{array}{ccc} F[x] & \xrightarrow{\varphi,\cong} & F[\alpha] \\ \subseteq\uparrow & & \subseteq\uparrow \\ F & \xrightarrow{\mathrm{id}_F} & F\ . \end{array}$$

Then φ_α is an F-isomorphism: $F[x] \overset{\cong}{\to} F[\alpha]$.

• (We didn't do) *Terminology:* An *F-homomorphism* is a field homomorphism $\varphi : K \to E$, where K/F and E/F are field extensions and φ is the identity homomorphism on F, that is, $\varphi|_F$ ($= \varphi$ restricted to F) is $\mathrm{id}_F : F \to F$.

$$\begin{array}{ccc} K & \xrightarrow{\varphi} & E \\ \subseteq\uparrow & & \subseteq\uparrow \\ F & \xrightarrow{\mathrm{id}_F} & F\ . \end{array}$$

• **Example 1.25.1:** For the ring $R = \frac{F[X]}{(p(X))} = F[x]$ of Theorem 1.25 with $F = \mathbb{F}_2$ and $p(X) = X^2 + X + 1$, we have (a) R has four elements: $R = \{0, 1, x, 1 + x\}$, and

(b) R is a field. We made addition and multiplication tables for R, using the fact that the coset $[X^2] = [X^2 + X^2 + X + 1] = [X + 1]$.

• **Two useful facts from ring theory:** Let R be a commutative ring.

(a) If I is an ideal of R, then $\frac{R}{I} = \{$ cosets $r + I$, where $r \in R\}$ is also a ring, with inherited $+, \cdot$ from R.

(b) if $\psi : R \to S$ is a ring homomorphism, if I is the kernel of ψ, and if $\pi : R \to \frac{R}{I}$ is the natural map $\pi(r) = r+I$, then there exists a one-to-one ring homomorphism $\varphi : \frac{R}{I} \to S$ such that $\varphi \circ \pi = \psi$. Pictorially, if we have maps ψ and π as shown,

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ {\scriptstyle\pi}\big\downarrow & & \\ \frac{R}{I} & & \end{array}$$

then there exists a diagonal map $\varphi : \frac{R}{I} \to S$ such that the diagram commutes. If, in addition, ψ is a surjection (onto), then φ is an isomorphism (one-to-one *and* onto).

• **Corollary 1.25.2:** (didn't do) If K/F and E/F are field extensions, $p(X) \in F[X]$ is irreducible and $\alpha \in K, \beta \in E$ satisfy $p(\alpha) = 0 = p(\beta)$, then there exists an F-isomorphism $\varphi : F(\alpha) \overset{\cong}{\to} F(\beta)$. To prove this, just take $\varphi = \varphi_\beta \circ {\varphi_\alpha}^{-1}$, where the isomorphisms φ_α and φ_β are given by part (2) of Theorem 1.25.

$$F(\alpha) = F[\alpha] \xrightarrow{\varphi_\alpha^{-1}} F[x] \xrightarrow{\varphi_\beta} F[\beta] = F(\beta)\,.$$

• **Examples 1.25.3:** For $F = \mathbb{R}$ and $p(X) = X^2 + 1$, the construction in Theorem 1.25 can be thought of as "creating a square-root for -1", or, equivalently, a root for $X^2 + 1$, by setting $R = \frac{\mathbb{R}[X]}{(X^2+1)}$. Similarly to create a square-root for 2, let $R = \frac{\mathbb{Q}[X]}{(X^2-2)}$.

• **Proposition 1.30:** Let E/F be a field extension. These conditions are equivalent:

(1) E/F is finite, i.e. $[E : F] < \infty$.

(2) E/F is algebraic and finitely generated over F, i.e. each element of E is algebraic and there exists a finite set $\alpha_1, \ldots, \alpha_n \in E$ such that $E = F(\alpha_1, \ldots, \alpha_n)$.

(3) There exists a finite set of algebraic (over F) elements $\alpha_1, \ldots, \alpha_n \in E$ such that $E = F(\alpha_1, \ldots, \alpha_n)$.

• **Corollary 1.31: Algebraic Tower of Fields Theorem** (Mentioned but didn't prove) Let $F \subseteq E \subseteq K$ be fields. If K is algebraic over E and E is algebraic over F, then K is algebraic over F.

• **Discussion of roots of unity:** Let p be a prime number. Let $\zeta_p = e^{\frac{2\pi i}{p}}$. Then ζ_p is a primitive p^{th} root of unity. In the complex plane with the x-axis real numbers and the y-axis the pure imaginary numbers, there are p roots of unity, evenly spaced as p points around the circle $x^2 + y^2 = 1$, including the point $x = 1, y = 0$. The minimal polynomial for ζ_p over $\mathbb{Q}$ is $p(X) = X^{p-1} + \cdots + X + 1$.

• **Lemma 1.41:** If p is a prime number then $p(X) = X^{p-1} + \cdots + X + 1$ is irreducible over $\mathbb{Q}$; hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

• Exercise: Find $[\mathbb{Q}(\zeta_{17}, 2^{\frac{1}{5}}) : \mathbb{Q}]$. Answer: 80.