DEFINITIONS AND THEOREMS FOR CHAPTER 20

Definition: Extension Fields
Let F be a field
If:
1. $F \subseteq E$ and
2. Operations of F are those of E *restricted* to F

Then: E is an *extension field* of F

Theorem 20.1 Fundamental Theorem of Field Theory
Let:
1. F be a field and
2. f(x) = non-constant polynomial $\in F[x]$

Then: $\exists$ an extension field E of F *such that* f(x) has a zero

Proof:

Showing there is an Extension Field

$\because$ F[x] = unique factorization domain *then* f(x) has an irreducible factor, say p(x)

Let $E = F / \langle p(x) \rangle$

By Corollary 1 of theorem 17.5: E is a field

Suppose $\phi : F \rightarrow E$ such that $\phi(a) = a + \langle p(x) \rangle$
Then ϕ is 1:1 and preserves both operations
Then E has a subfield *isomorphic* to F

Let coset be $(a + \langle p(x) \rangle)$, $a \in F$ *then:* can think of E as containing F

Showing f(x) has a zero

To show p(x) has a zero in E:
Let $p(x) = a_n x^n + \ldots\ldots + a_0$

Then $p(x + \langle p(x) \rangle) = \ldots\ldots$ (see text) $= p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle$

Then in E, $x + \langle p(x) \rangle$ is a zero of p(x)

Definition: Splitting Field
Let:
1. E be an extension field of F
2. $f(x) \in F[x]$

If f(x) can be factored as a product of linear factors in E[x] *then* f(x) splits in E

If f(x) splits in E but not in no proper subfield of E, E = splitting field for f(x) over F

Notation:
Let:

1. F be a field
2. $a_1, \dots, a_n$ be elements of some extension E of F

- $F(a_1, \dots, a_n)$ = smallest subfield of E *that* contains F and $\{a_1, \dots, a_n\}$
  = intersection of all subfields of E that contain F and $\{a_1, \dots, a_n\}$

Suppose:

1. $f(x) \in F[x]$
2. $f(x) = b(x - a_1) \dots\dots (x - a_n)$

Over some extension field E of F

Then: $F(a_1, \dots, a_n)$ is a splitting field for f(x) over F in E

Theorem 20.2 Existence of Splitting Fields
Let:

1. F be a field
2. f(x) = non-constant element of F[x]

Then $\exists$ a splitting field E for f(x) over F

Proof: (induction on deg f(x))

Base Case: deg f(x) = 1 *then* f(x) is linear

Suppose:
Statement is true for all fields and all polynomials (degree of polynomial is less than deg f(x))

By 20.1, there is an extension E of F in which f(x) has a zero, say a_1
$\Rightarrow$ can write $f(x) = (x - a1)g(x)$, $g(x) \in E[x]$

deg g(x) < deg f(x)
$\Rightarrow$ there is a field K that contains: E and $\{ a_1, \dots, a_n \}$ = all the zeros of g(x)

Then: $F(a_1, \dots, a_n)$ = splitting field for f(x) over F

Theorem 20.3 $F(a) \approx F[x] / \langle p(x) \rangle$
Let:

1. F be a field
2. $p(x) \in F[x]$ be irreducible over F

i. If 'a' is a zero of p(x) in some extension E of F *then* $F(a) \cong F[x] / \langle p(x) \rangle$
ii. If deg p(x) = n, *then* every member of F(a) can be expressed as:
   - $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \dots + c_1a + c_0$, where $c_0, c_1, \dots, c_{n-1} \in F$

Proof:

Showing that: $F(a) \approx F[x] / \langle p(x) \rangle$

Consider $\phi : F[x] \rightarrow F(a)$ *such that* $\phi(f(x)) = f(a)$

Then: ϕ is a ring homomorphism

Claim: $\text{Ker}\ \phi = \langle p(x) \rangle$

1. Since $p(a) = 0 \quad \Rightarrow \quad \langle p(x) \rangle \subseteq \text{Ker}\ \phi$

2. Theorem 17.5: $\langle p(x) \rangle$ is a maximal ideal in $F[x]$

   Since $f(x) = 1$ is not in Ker ϕ, so Ker $\phi \neq F[x]$
   $\Rightarrow$ Ker $\phi = \langle p(x) \rangle$

Corollary 1 of 17.5:
F a field, p(x) irreducible polynomial over F, then $F[x] / \langle p(x) \rangle$ is a field

Corollary + First Isomorphism Theorem $\Rightarrow \phi(F[x])$ is a subfield of F(a)

Since $\phi(F[x])$ contains: {F, a} <u>and</u> since F(a) is the smallest such field
$\Rightarrow F[x] / \langle p(x) \rangle \approx \phi(F[x]) = F(a)$

Corollary F(a) ≈ F(b)
Let:

1. F be a field
2. $p(x) \in F[x]$ is irreducible over F
3. E and E′ are some extension fields of F

<u>If</u> 'a' is a zero of p(x) in E <u>and</u> 'b' is a zero of p(x) in E′ , *then* the fields $F(a) \approx F(b)$

Lemma
Let

1. (1) & (2) from above corollary hold, *and*
2. a = zero of p(x) in some extension field of F

<u>If:</u>

1. $\phi : F \rightarrow F'$ is an isomorphism *and*
2. b = zero of $\phi(p(x))$ in some extension field F′

<u>Then:</u> $\exists$ an iso. from $F(a) \rightarrow F'$ (b) that agrees with ϕ on F and carries $a \rightarrow b$

[Proof: see lecture notes]

Theorem 20.4 Extending $\phi : F \to F'$

Let:

1. ϕ be an isomorphism from a field F to a field F'
2. $f(x) \in F[x]$

If E is a splitting field for f(x) over F *and* E' is a splitting field for $\phi(f(x))$ over F

Then: $\exists$ an isomorphism from $E \to E'$ that agrees with ϕ on F

[Proof: (Induction on deg f(x)) : see lecture notes]

Corollary: Splitting Fields are Unique

Let:

1. F be a field
2. $f(x) \in F[x]$

Then: any two *splitting fields* of f(x) over F are isomorphic

Theorem 20.5 Criterion for Multiple Zeros

A polynomial f(x) over a field F has a multiple zero in some extension E

$\Leftrightarrow$ f(x) and $f'(x)$ have a common factor of positive degree in F[x]

Theorem 20.6 Zeros of an Irreducible

Let f(x) be an irreducible polynomial over a field F.

Char F = 0 $\Rightarrow$ f(x) has no multiple zeros

Char F $\neq$ 0 $\Rightarrow$ f(x) has multiple zero *only if* it is of the form $f(x) = g(x^p)$, for some $g(x) \in F[x]$

Proof:

Theorem 20.5: f(x) has multiple zero $\Rightarrow$ $\{f(x), f'(x)\}$ has a *common divisor* of positive degree in F[x]

But only divisor of f(x) of positive degree = f(x) ; itself

And deg $f'(x)$ < deg f(x)

So: $\because$ $f(x) \mid f'(x)$, but a field cannot divide a poly. of smaller degree

$\Rightarrow f'(x) = 0$

Notice: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

So: $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$

So: $f'(x) = 0$ *only when* $ka_k = 0$ for $k = 1, \ldots, n$

Case 1: Suppose Char F = 0

$\Rightarrow f(x) = a_0$, thus f(x) not irreducible

$\Rightarrow$ contradicts hypothesis that f(x) is irreducible over F

$\Rightarrow$ f(x) has no multiple zeros

Case 2: Suppose Char F = p $\neq$ 0, Thus $a_k = 0$ *when* $p \nmid k$

$\Rightarrow a_k x^k$ appears in $a_n x^n + \ldots + a_1 x + a_0$ *only if* x^k is of the form $x^{pj} = (x^p)^j$

$\Rightarrow f(x) = g(x^p)$

Example: $f(x) = x^{4p} + 3x^{2p} + x^p + 1$ then: $g(x) = x^4 + 3x^2 + x + 1$

Definition: Perfect Field
A field F is called *perfect* if:
1. Char F = 0 *or*
2. $F^p = \{a^p \mid a \in F\} = F$

Theorem 20.7: Every finite Field is *perfect*

Theorem 20.8: Criterion for No Multiple Zeros
If f(x) is an *irreducible* polynomial over a *perfect* field F, then f(x) has no multiple zeros

Theorem 20.9: Zeros of an Irreducible over a Splitting Field
Let:
1. f(x) be an irreducible polynomial over a field F
2. E be a splitting field of f(x) over F

Then: *all* the *zeros* of f(x) in E have the same multiplicity

Corollary: Factorization of an Irreducible over a splitting field
See text book page: 364