Lecture 13

Let $f(x) \in F[x]$, $\deg f(x) = n \geq 1$, F field, K ext. field of F.

Def: The polynomial $f(x) \in F[x]$ splits over K if it can be written $f(x) = c(x-u_1)(x-u_2)\cdots(x-u_n)$, $c \in F$, $u_i \in K$.

K is a splitting field of $f(x)$ over F if

$$\begin{cases} ① & f(x) \text{ splits over } K \\ ② & K = F(u_1, u_2, \dots, u_n) \quad (K \text{ smallest field containing } F \text{ and all } u_i) \end{cases}$$

Ex: Splitting field of x^2+1 over $\mathbb{R}$ is $\mathbb{R}(i,-i) = \mathbb{R}(i) = \mathbb{C}$ (since $x^2+1 = (x-i)(x+i)$), but over $\mathbb{Q}$ it is $\mathbb{Q}(i,-i) = \mathbb{Q}(i) \subsetneq \mathbb{C}$.

Ex: Splitting field of $x^4 - x^2 - 2 = (x^2-2)(x^2+1)$ over $\mathbb{Q}$ is $\mathbb{Q}(\pm\sqrt{2}, \pm i) = \mathbb{Q}(\sqrt{2}, i)$.

Ex: A splitting field of a polynomial of degree is always equal to the base field F:

$$f(x) = ax+b = a(x + a^{-1}b) \text{ and } F(\underbrace{-a^{-1}b}_{\in F}) = F.$$

Repetition: $p(x) \in F[x]$ irreducible

$\Rightarrow F[x]/(p(x))$ extension field of F containing a root u of $p(x)$.

u is algebraic over F and $F(u) \cong F[x]/(p(x))$.

> **Theorem:** Let $f(x) \in F[x]$, $\deg f(x) = n \geq 1$. Then there exists a splitting field K of $f(x)$ over F with $[K:F] \leq n!$.

Proof: Induction over $\deg f(x)$:

$n=1$: $K = F$ and $[K:F] = [F:F] = 1 \leq 1!$ (see example above)

$n>1$: Let $p(x)$ be an irr. factor of $f(x)$ and consider $F[x]/(p(x)) \cong F(u)$ above. By the factor theorem in $F(u)[x]$ we have

$$f(x) = (x-u)g(x), \quad g(x) \in F(u)[x].$$

By induction there exists a splitting field $K = F(u)(v_1, v_2, \dots, v_{n-1})$ of $g(x)$ over $F(u)$ and $[K:F(u)] \leq (n-1)!$ The field $K = F(u, v_1, v_2, \dots, v_{n-1})$ contains all the roots of $f(x)$ and thus is a splitting field of $f(x)$ over F.

Furthermore

$$[K:F] = [K:F(u)][F(u):F] = [K:F(u)] \cdot \deg p(x) \leq$$
$$\leq (n-1)! \cdot n = n! \qquad \square$$

> **Theorem:** Any two splitting fields of $f(x)$ over F are isomorphic.

Proof: See book.

- Study yourself: Concept of normal extension and Theorem 10.15.

Def: A field K withe the property that every $f(x) \in K[x]$ splits over K is called algebraically closed.

Ex: $\mathbb{C}$ is alg. closed (fund. theorem of algebra)

If $K \supseteq F$ is an algebraic extension and K is alg. closed, then K is called the algebraic closure of F (exists and is unique up to isomorphism).

Ex: $\mathbb{C}$ alg. closure of $\mathbb{R}$

$\mathbb{C}$ is not alg. closure of $\mathbb{Q}$ ($\mathbb{C}$ not algebraic over $\mathbb{Q}$)

(The alg. closure of $\mathbb{Q}$ is the field of alg. numbers)

- Chapter 10.5 not included in the course.

Let $(R,+,\cdot)$ be a ring with unity. As usual, we write

$$mc = \underbrace{c + c + \cdots + c}_{m}, \quad m \in \mathbb{Z}, c \in R.$$

Def: If $m>0$ is the smallest integer such that $m \cdot 1_R = 0_R$, then we say that R has characteristic m, and write $\operatorname{char} R = m$. If $m \cdot 1_R \neq 0_R$ for all $m>0$, then $\operatorname{char} R = 0$.

Ex: $\operatorname{char} \mathbb{Q} = 0$, $\operatorname{char} \mathbb{Z}_6 = 6$, $\operatorname{char} \mathbb{Z}_6[x] = 6$

Note: $\operatorname{char} R = m \Leftrightarrow$ subgroup $\langle 1_R \rangle$ has order m in the group $(R,+)$

> **Lemma:** R integral domain $\Rightarrow \operatorname{char} R = p$, p prime or $\operatorname{char} R = 0$

Proof: Assume $\operatorname{char} R = n \neq 0$ and let $n = kt$, $1 < k,t < n$.

Then
$$(k \cdot 1_R) \cdot (t \cdot 1_R) = (\underbrace{1_R + 1_R + \cdots + 1_R}_{k})(\underbrace{1_R + 1_R + \cdots + 1_R}_{t}) =$$
$$= \underbrace{1_R + 1_R + \cdots + 1_R}_{k \cdot t} = (kt) \cdot 1_R = n \cdot 1_R = 0_R$$

$\underset{\text{int. dom.}}{\Rightarrow}$ $k \cdot 1_R = 0_R$ or $t \cdot 1_R = 0_R$, contradiction. $\square$

> **Lemma:** Assume $\operatorname{char} R = n$. Then $k \cdot 1_R = 0_R \Leftrightarrow n \mid k$.

Proof: Follows from corr. theorem for groups.

Theorem: ① $P = \{k \cdot 1_R \,;\, k \in \mathbb{Z}\}$ is a subring of R

② $\operatorname{char} R = 0 \Leftrightarrow P \cong \mathbb{Z}$

③ $\operatorname{char} R = n \Leftrightarrow P \cong \mathbb{Z}_n$

Proof: $f:\mathbb{Z}\to R$, $f(k)=k\cdot 1_R$ is a ringhom. (check!)

① Since $P \cong \operatorname{Im} f$ it follows that P is a subring

② F.I.Th $\Rightarrow$ $P \cong \operatorname{Im} f \cong \mathbb{Z}/\ker f$

Since char $R=0$, we have $\ker f=\{0\}$,

and $P\cong \mathbb{Z}/\{0\}\cong\mathbb{Z}$

③ char $R=n$ $\Rightarrow$ $\ker f=(n)$ according to lemma, and

$$P=\operatorname{Im} f\cong \mathbb{Z}/\ker f=\mathbb{Z}/(n)\cong\mathbb{Z}_n \qquad \square$$

$\boxed{\textbf{Corollary: } F \text{ finite field} \Rightarrow \text{char } F=p,\ p \text{ prime}}$

Proof: Since F is finite it cannot contain $\mathbb{Z}$ as a subring $\Rightarrow$ char $F\neq 0$. Since F field $\Rightarrow$ F int. domain we must have char $F=p$, p prime. $\square$

If F field, char $F=p$, then $P\cong\mathbb{Z}_p$ is the smallest subfield of F (note that every subfield contains 1_F, and thus entire P) called the <u>prime subfield</u> of F.

<u>Note</u>: If char $F=0$, then prime subfield is $\underline{\mathbb{Q}}$!

<u>Theorem</u>: F finite field $\Rightarrow$ $|F| = p^n$, (no. elements)

where $p=\text{char } F$ and $n=[F:\mathbb{Z}_p]$.

Proof: F finite $\Rightarrow$ F fin. gen. vectorspace over $P\cong\mathbb{Z}_p$

$\Rightarrow$ F has a basis $u_1,u_2,\dots,u_n$ over $\mathbb{Z}_p$

$\Rightarrow$ every $a\in F$ can be uniquely written

$$a=c_1u_1+c_2u_2+\dots+c_nu_n,\quad c_i\in\mathbb{Z}_p$$

$$\Rightarrow |F|=\underbrace{p\cdot p\cdots p}_{n}=p^n \qquad \square$$

We can now conclude that there are no fields with e.g. 75 elements, since $75\neq p^n$. Conversely, is it true that there are fields of every order p^n, p prime, $n\geq 1$?

Note that if $f(x)\in\mathbb{Z}_p[x]$ is irreducible of degree n, then the field $\mathbb{Z}_p[x]/(f(x))$ has p^n elements.

(But we do not know if there are irr. polynomials in $\mathbb{Z}_p[x]$ of arbitrary degree.)

$\boxed{\begin{array}{l}\textbf{Lemma: } R \text{ comm. ring with identity, char } R=p\ (p \text{ prime}).\\ \text{Then } (a+b)^{p^n}=a^{p^n}+b^{p^n} \text{ for all } a,b\in R.\end{array}}$

Proof: Induction on n:

<u>$n=1$</u>: $(a+b)^p=\sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k$, and $\binom{p}{k}=\frac{p!}{k!(p-k)!}\equiv 0$ modulo p (exercise) for $1\leq k\leq p-1$, so

$(a+b)^p\equiv a^p+b^p \pmod p$ $\Rightarrow$ $(a+b)^p=a^p+b^p$ in any ring with char. p.

<u>$n=k+1$</u>: $(a+b)^{p^{k+1}}=\left((a+b)^{p^k}\right)^p \overset{\text{ind.}}{=} \left(a^{p^k}+b^{p^k}\right)^p \overset{\text{ind.}}{=}$

$$=\left(a^{p^k}\right)^p+\left(b^{p^k}\right)^p=a^{p^{k+1}}+b^{p^{k+1}} \qquad \square$$

$\boxed{\begin{array}{l}\textbf{Theorem: } F \text{ extension field of } \mathbb{Z}_p,\ n\geq 1. \text{ Then}\\ |F|=p^n \Leftrightarrow F \text{ is a splitting field of } f(x)=x^{p^n}-x\\ \text{over } \mathbb{Z}_p\end{array}}$

Proof: $\Rightarrow$) $F^*=F\setminus\{0\}$ is a multiplicative group of order p^n-1 $\Rightarrow$ $a^{p^n-1}=1$ for all $a\in F^*$

$\Rightarrow$ $a^{p^n}=a$ for all $a\in F^*$, ~~And since also a=0~~ as well as for $a=0$

$\Rightarrow$ $a^{p^n}=a$ for all $a\in F$ $\Rightarrow$ every element of F is a root of $f(x)=x^{p^n}-x$. Since $|F|=p^n$ and $\deg f=p^n$, $F=\{\text{roots of } f(x)\}$ $\Rightarrow$ F is the splitting field of f

$\Leftarrow$) Let $E=\{\text{roots of } f(x)\}\subseteq F$ and show

① <u>E field</u>: <u>$0,1\in E$</u> OK

$a,b\in E$ $\Rightarrow$ $(a+b)^{p^n}=a^{p^n}+b^{p^n}=a+b$ $\Rightarrow$ $\underline{a+b\in E}$

p odd: $(-a)^{p^n}=-a^{p^n}=\underline{-a}$

$p=2$: $(-a)^{2^n}=a^{2^n}=a=\underline{-a}$ $\Rightarrow$ $\underline{-a\in E}$

$(ab)^{p^n}=a^{p^n}b^{p^n}=ab$ $\Rightarrow$ $\underline{ab\in E}$

$(a^{-1})^{p^n}=(a^{p^n})^{-1}=a^{-1}$ $\Rightarrow$ $\underline{a^{-1}\in E}$

② $\underline{E=F}$, since F smallest subfield containing $\mathbb{Z}_p$ and all roots of f. ($1\in E \Rightarrow k\cdot 1\in E \Rightarrow \mathbb{Z}_p\subseteq E$)

③ $\underline{|E|=p^n}$: Let $c\neq 0$ be a root of $x^{p^n}-x=x(x^{p^n-1}-1)$

$$\Rightarrow x^{p^n-1}-1=(x-c)\underbrace{(x^{p^n-2}+cx^{p^n-3}+\dots+c^{p^n-3}x+c^{p^n-2})}_{=g(x)}=(x-c)g(x)$$

We have $g(c)=c^{p^n-2}+c^{p^n-2}+\dots+c^{p^n-2}=(p^n-1)c^{p^n-2}\neq 0$

(since char $F=p$ and $p\nmid p^n-1$)

$\Rightarrow$ c simple root $\Rightarrow$ all roots distinct,

and since $\deg f(x)=p^n$ $\Rightarrow$ $|E|=p^n$ $\square$

$\boxed{\textbf{Corollary: } \text{There are fields of every order } p^n.}$

$\boxed{\textbf{Corollary: } \text{Two finite fields of the same order are isomorphic.}}$

Proof: Order is p^n and splitting fields are unique. $\square$

$\boxed{\begin{array}{l}\textbf{Theorem: } \text{If } F \text{ is a subfield of a finite field } K,\\ \text{then } K \text{ is a simple extension of } F.\end{array}}$

Proof: $(K^*,\cdot)$ is a finite group $\overset{\text{Th.7.15.}}{\Rightarrow}$ $(K^*,\cdot)=\langle u\rangle$ is cyclic $\Rightarrow$ $K=F(u)$. $\square$

~~Corollary: There exists F ⊇ Z_p with |F|=p^n~~

Corollary: There is an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$ for all $n \geq 1$.

Proof: There exists $F \supseteq \mathbb{Z}_p$ with $|F| = p^n$ (prev. theorem)

$\Rightarrow$ $F = \mathbb{Z}_p(u)$ for some $u \in F$. Minimal polynomial of u in $\mathbb{Z}_p[x]$ is irregular of degree $[F : \mathbb{Z}_p] = n$. $\square$