Prof. Salil Vadhan

Lecture Notes 19
November 17, 2010

## 1 Extension Fields

- Reading: Parts of Ch. 20, 21.
- Today we will study how to build "larger" fields from smaller fields.

Def: For fields $E, F, E$ is an extension field of $F$ iff $F$ is (isomorphic to) a subfield of $E$.

- We will focus on starting with a field $F$ and adjoining a single element $a$ to $F$. Of course, once we add an element $a$, we must add other elements to have closure under addition and multiplication and to have multiplicative inverses. For example, we must add the powers of $a$, linear combinations of those powers, ratios of elements, etc.
- We have already seen one way of adding an element: adding a new variable $x$ to get the polynomial ring $F[x]$ and then reducing modulo an irreducible polynomial:

Thm 20.1: If $p(x) \in F[x]$ is an irreducible polynomial, then $F[x] /\langle p(x)\rangle$ is an extension field of $F$. Moreover $p$ has a root in $F[x] /\langle p(x)\rangle$, namely $x$ itself (or, more precisely, the coset $x+\langle p(x)\rangle)$.

## - Example:

$-\mathbb{Z}_{2}[x] /\left\langle x^{3}+x^{2}+1\right\rangle$.

- How to compute inverses in $F[x] /\langle p(x)\rangle$ ?
- We can also add a new element $x$ that doesn't satisfy any polynomial equation over $F$ :

Def: For a field $F$, the field $F(x)$ of rational functions over $F$ consists of ratios $f(x) / g(x)$ of polynomials $f(x), g(x) \in F[x]$ such that $g(x) \neq 0$, where we treat two ratios $f_{1}(x) / g_{1}(x)$ and $f_{2}(x) / g_{2}(x)$ as equal iff $f_{1}(x) g_{2}(x)=f_{2}(x) g_{1}(x)$, and addition and multiplication is done as you would expect.

- It can be verified that $F(x)$ a field.
- More generally we can take any integral domain $R$ (like $F[x]$ or $\mathbb{Z}$ ) and obtain a "field of quotients" that contains $R$ (like $F(x)$ or $\mathbb{Q}$ ).
- If we already have a field $E$ that contains $F$, then we can also adjoin any element of $E$ to $F$ :

Def: Let $E$ be an extension field of $F$, and $a \in E$. Then $F(a)$ is defined to be the smallest subfield of $E$ containing $F$ and $a$, namely $F(a)=\{f(a) / g(a): f, g \in F[x], g(a) \neq 0\}$. (Can be verified that this is a field.)

- The use of parenthesis in $F(a)$ indicates that we are looking at all rational functions $f(x) / g(x)$ applied to $a$ in contrast to $F[a]=\{f(a): f \in F[x]\}$, where we only look at polynomial functions applied to $a$. Using rational functions ensures that we get multiplicative inverses, though, as we'll see, in some cases it is not necessary.
- Example: $\mathbb{Q}(\sqrt{5})$
- Now we will see that this method of getting extension fields (adjoining a specific element $a$ ) is equivalent to the previous ones (where we adjoined an abstract element $x$ ). Whether we get something of the form $F(x)$ or of the form $F[x] /\langle p(x)\rangle$ depends on properties of the element $a$.
- Def: Let $E$ be an extension field of $F, a \in E$. We say that $a$ is algebraic over $F$ if it is the root of a nonzero polynomial in $F[x]$. Otherwise we say that $a$ is transcendental over $F$. If $a$ is algebraic, the minimal polynomial for $a$ is the monic polynomial of lowest degree in $F[x]$ that has $a$ as a root.


## - Examples and Nonexamples:

$-\sqrt{5}$ over $\mathbb{Q}$.
$-i$ over $\mathbb{R}$.
$-\pi$ over $\mathbb{Q}$.

- Thm 21.1: Let $E$ be an extension field of $F$ and let $a \in E$ be transcendental over $F$. Then $F(a) \cong F(x)$. Moreover the isomorphism is the identity on $F$ and takes $x$ to $a$.

Proof: in Gallian

- Thms 20.3,21.1: Let $E$ be an extension field of $F$, and let $a \in E$ be algebraic over $F$. Then:

1. The minimal polynomial $p(x)$ for $a$ over $F$ is irreducible.
2. $F(a) \cong F[x] /\langle p(x)\rangle$. (Moreover, the isomorphism is the identity on $F$ and takes the (coset containing) $x$ to $a$.)
3. $F(a)=\left\{c_{0}+c_{1} a+c_{2} a^{2}+\cdots+c_{n-1} a^{n-1}: c_{0}, c_{1}, \ldots, c_{n-1} \in F\right\}$, where $n=\operatorname{deg}(p)$.

## Proof:

- Corollary: If $a \in E$ and $a^{\prime} \in E^{\prime}$ have the same minimal polynomial, then $F(a) \cong F\left(a^{\prime}\right)$. (Moreover, the isomorphism is the identity on $F$ and takes $a$ to $a^{\prime}$.)


## - Examples:

$-\mathbb{R}(i) \cong \mathbb{R}[x] /\left\langle x^{2}+1\right\rangle \cong \mathbb{R}(-i)$.
$-\mathbb{Q}(\sqrt{5}) \cong \mathbb{Q}[x] /\left\langle x^{2}-5\right\rangle \cong \mathbb{Q}(-\sqrt{5})$.

## 2 Splitting Fields

- Def: Let $E$ be an extension field of $F$ and $f(x) \in F[x]$. We say that $f(x)$ splits in $E$ iff $f(x)$ can be factored into linear factors in $E[x]$. That is, $f(x)=c\left(x-a_{1}\right)\left(x-a_{2}\right) \cdots\left(x-a_{k}\right)$ for $c, a_{1}, \ldots, a_{k} \in E$ (possibly with repetitions). $E$ is a splitting field for $f(x)$ over $F$ iff $f(x)$ splits in $E$ but in no proper subfield $E^{\prime}$ such that $F \subseteq E^{\prime} \subsetneq E$.
- Thm 20.2+: For every polynomial $f(x) \in F[x]$, there exists a splitting field $E$ for $f(x)$ over $F$. Moreover every two splitting fields for $f(x)$ are isomorphic.

Proof idea: (details in book)

- Example: Splitting field of $x^{8}-1$ over $\mathbb{Q}$.

