Algebra 1-4-2019

For each prime p and $n \in \mathbb{N}$ there exists a unique field $\mathbb{F}$ with $|\mathbb{F}| = p^n$.
Moreover if $\mathbb{F}$ is a finite field, then $\exists$ p prime and $n \geq 1$ such that $|\mathbb{F}| = p^n$.

$A \subset R$

- ideal; additive group s.t. $rA \subset A$
- maximal ideal $A \subset B \subset R$
  $\Rightarrow A = B$ or $B = R$
- If $1 \in R$, $A \subset R$ is maximal ideal:
  R/A is a field (if and only if)
- $R/A = \{ r + A \mid r \in R \}$
  $(r+A)+(s+A) = r+s+A$
  $(r+A).(s+A) = rs + A$

Consider $R = \mathbb{R}[x] = \{ r(x) \mid r(x)$ polynomial $r_0 + r_1 x + r_2 x^2 + \dots + r_n x^n,$ $r_i \in \mathbb{R}, n \geq 0 \}$.

Let $A = \langle x^2+1 \rangle = \{ (x^2+1)a(x) \mid a(x) \in \mathbb{R}[x] \}$.

Claim A is maximal ideal
$\Rightarrow \mathbb{R}[x]/(x^2+1)$ is a field.

$= \{ r(x) + (x^2+1) \mid r(x) \in \mathbb{R}[x] \}$.

$= \{ r_0 + r_1 x + (x^2+1) \mid r_0, r_1 \in \mathbb{R} \}$. ←

namely: $r(x) = \underbrace{q(x).(x^2+1)}_{\in A} + s(x)$ $\deg s(x) < 2$

$\Rightarrow r(x) + A = s(x) + A$

$(r_0+r_1x+A)+(s_0+s_1x+A) = (r_0+s_0)+(r_1+s_1)x+A$

$(r_0+r_1x+A)(s_0+s_1x+A) = r_0s_0 + (r_0s_1+r_1s_0)x + r_1s_1x^2 + A$

notice that $A = (x^2+1)$

$\Rightarrow \quad -1+A = x^2+A$ (because $1+x^2 \in A$)

$\hookrightarrow (r_0s_0 - r_1s_1) + (r_0s_1+r_1s_0)\cdot x$

Theorem * Let $\mathbb{F}$ be a field and $R = \mathbb{F}[x]$; $A = (p(x))$ $p(x) \in \mathbb{F}[x]$
then A is maximal ideal $\Leftrightarrow$ $p(x)$ is irreducible

Def. $p(x) \in \mathbb{F}[x]$ is irreducible if $p(x) = f(x)\cdot g(x)$ then either $\deg f(x) = \deg p(x)$ or $\deg g(x) = \deg p(x)$

Thm. If $\deg p(x) = 2$ or 3 then $p(x)$ is irreducible $\Leftrightarrow$ $p(a) \neq 0$ $\forall a \in \mathbb{F}$.

proof of Theorem *

$\Rightarrow$ Suppose $A = (p(x))$ is maximal
assume that $p(x) = f(x)\cdot g(x)$
$\deg f(x) < \deg p(x)$ $\deg g(x) < \deg p(x)$
then $(p(x)) \subsetneq (f(x)) \subsetneq \mathbb{F}[x]$ ξ

$\Leftarrow$ $f(x)$ irreducible, suppose $(f(x)) \subseteq \mathcal{B} \subseteq \mathbb{F}[x]$
$\mathcal{B} = (g(x))$ with $\deg g(x)$ minimal among elts. of $\mathcal{B}$.

$$(p(x)) \subset \underset{\| \; (f(x))^{*}\text{ see below}}{\mathcal{B}} \subset \mathbb{F}[x]$$

$p(x) \in (f(x)) \Rightarrow p(x) = q(x)f(x)$

$\Rightarrow$ either $q(x)$ has degree $\deg p(x)$

$\Rightarrow f(x) = c \in \mathbb{F} \setminus \{0\} \Rightarrow \mathcal{B} = \mathbb{F}[x]$

or $\deg f(x) = \deg p(x) \Rightarrow \mathcal{B} = \langle p(x) \rangle$

□

$x^2+1 \in \mathbb{R}[x]$ is irreducible because it has no zero's.

$\Rightarrow \mathbb{R}[x]/\langle x^2+1 \rangle$ is a field, in fact isomorphic to $\mathbb{C}$

Let $p(x) \in \mathbb{F}[x]$ be irreducible and $\deg p(x) = n$.
then any element in the field $\mathbb{F}[x]/\langle p(x) \rangle$ is represented as:

$$r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1} + \langle p(x) \rangle$$

$\Rightarrow$ n dimensional vector space $r_i \in \mathbb{F}$

$p(x) = p_0 + p_1 x + \cdots + p_{n-1} x^{n-1} + x^n$

Then $x^n + \langle p(x) \rangle = -p_0 - p_1 x - \cdots - p_{n-1} x^{n-1} + \langle p(x) \rangle$

($r_0 + r_1 x + \langle x^2+1 \rangle : \mathbb{R}[x]/\langle x^2+1 \rangle$ is a vector space over $\mathbb{R}$ with basis $1 + \langle x^2+1 \rangle$, $x + \langle x^2+1 \rangle$
$\Rightarrow$ dimension 2.)

Let $\mathbb{F}$ be a finite field
$\mathrm{char}(\mathbb{F}) = p$ p prime
$\Rightarrow 1, \underbrace{1+1}_{2}, \underbrace{1+1+1}_{3}, \ldots, \underbrace{1+\cdots+1}_{p-1}, \underbrace{1+\cdots+1}_{p} = 0$
$\Rightarrow \mathbb{Z}_p$ is a subfield of $\mathbb{F}$.
$\Rightarrow \mathbb{F}$ is a vector space w.r.t. $\mathbb{Z}_p$
$\Rightarrow$ there exists a basis, say, $b_1, \ldots, b_n \in \mathbb{F}$
$\Rightarrow a \in \mathbb{F} \Rightarrow a = \alpha_1 b_1 + \alpha_2 b_2 + \cdots + \alpha_n b_n$
$\alpha_i \in \mathbb{Z}_p$ same as

$\Rightarrow |\mathbb{F}| = p^n$

$R = \{ a+bi \mid a, b \in \mathbb{Z}_3 \}$ is int. dom., finite
$\Rightarrow R$ is a field $\quad i^2 = -1$

notice that x^2+1 is irreducible in $\mathbb{Z}_3[x]$.
$\mathbb{Z}_3(x)/_{\langle x^2+1 \rangle}$ is a field;

$r_0 + r_1 x + \langle x^2+1 \rangle$

Generally: find irreducible $p(x) \in \mathbb{Z}_p[x]$
with $\deg p(x) = n$
then $|\mathbb{Z}_p(x)/_{\langle p(x) \rangle}| = p^n$

however
- hard to find
- uniqueness cannot easily be concluded in this approach

What about $\mathbb{Z}_2[x]/_{\langle x^2+1 \rangle}$ is not a field
because $x^2+1 = (x+1)(x+1)$

*) $B \subset \mathbb{F}[x]$ ideal ($\mathbb{F}$ field) $\Rightarrow$
$B = \langle f(x) \rangle$, $f(x) \in \mathbb{F}[x]$, in other
words $\mathbb{F}[x]$ is principal ideal domain
proof Take for $f(x) \in B$ any nonzero
polynomial of minimal degree and
let $b(x) \in B$; write $b(x) = q(x)f(x) + r(x)$,
$\deg r(x) < \deg f(x)$. $b(x) \in B$, $f(x) \in B \Rightarrow$
$r(x) \in B$, since $\deg r(x) < \deg f(x)$ and
$\deg f(x)$ is minimal among all
nonzero polynomials in B it follows
that $r(x) = 0$ (zero polynomial) and

hence indeed $\mathcal{D} = (f(n))$.