PROPOSITION: A domain R (and hence every field) has characteristic either a prime p (like $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) or characteristic 0 (like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$)

proof: Given a domain R, if characteristic is $n \neq 0$ and n is not prime, say $n = n_1 n_2$

then $0 = \underbrace{1+1+\cdots+1}_{n \text{ times}} = \underbrace{(1+\cdots+1)}_{n_1 \text{ times}} \underbrace{(1+\cdots+1)}_{n_2 \text{ times}}$ (use distributivity)

forces either $\underbrace{1+\cdots+1}_{n_1} = 0$, i.e. R has smaller characteristic!

or $\underbrace{1+\cdots+1}_{n_2}$ ∎

1/30/2019

COROLLARY: Every finite field $\mathbb{F}$ has characteristic a prime p, and $|\mathbb{F}| = p^d$ for some $d \geq 1$.

proof: In $\mathbb{F}$, the sequence $1, \frac{1+1}{2}, \frac{1+1+1}{3}, \cdots$ must eventually repeat since $|\mathbb{F}| < \infty$, and if $m = n$ for some $m < n$ then $-m+m = -m+n$, so $\mathbb{F}$ has characteristic not 0, $\quad (0)$

which must be a prime p by PROP above.

We claim then that every $\alpha \in \mathbb{F}$ has $p\alpha := \underbrace{\alpha+\alpha+\cdots+\alpha}_{p \text{ times}} = 0$

since $p\alpha = (1+1+\cdots+1)\alpha = 0 \cdot \alpha = 0$

and therefore we can make $\mathbb{F}^+ = (\mathbb{F}, +)$ into a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{(p-1)}\}$

by defining the scaling $\mathbb{F}_p \times \mathbb{F} \longrightarrow \mathbb{F}$

$(\bar{m}, \alpha) \longmapsto \bar{m} \cdot \alpha = \underbrace{\alpha+\cdots+\alpha}_{m \text{ times}}$

(Checking well-defined-ness is the trickiest part; rest is easy)

$\bar{m}_1 = \bar{m}_2 \Rightarrow \bar{m}_1 \cdot \alpha = \bar{m}_2 \cdot \alpha$

(11)

The $\mathbb{F}_p$-vector space $\mathbb{F}$ is finite-dimensional since $\mathbb{F}$ is spanned over $\mathbb{F}_p$ by $\mathbb{F}$ itself (!).

So if $\dim_{\mathbb{F}_p}(\mathbb{F}) = d$, i.e. $\mathbb{F}$ has some $\mathbb{F}_p$-basis $\alpha_1, \ldots, \alpha_d \in \mathbb{F}$

then $\mathbb{F} \cong (\mathbb{F}_p)^d$ as $\mathbb{F}_p$-vector spaces,

$$c_1\alpha_1 + \ldots + c_d\alpha_d \longleftrightarrow \begin{bmatrix} c_1 \\ \vdots \\ c_d \end{bmatrix}$$

so $|\mathbb{F}| = |(\mathbb{F}_p)^d| = p^d$ ∎

(Smallest non-$\mathbb{F}_p$)

EXAMPLE: $\mathbb{F}_{2^2} = \mathbb{F}_4 := \{0, 1, \alpha, \underbrace{\alpha+1}_{=\alpha^2}\}$ with $\underbrace{\alpha}_{=\alpha^3}$

$\cong (\mathbb{F}_2)^2$ with $\mathbb{F}_2$-basis $\{1, \alpha\}$

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

×	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

but it's not clear until later how we built this, or why it's a field!

To see why finite fields $\mathbb{F}$ have $\mathbb{F}^\times$ cyclic, and for many other purposes, we need to understand easy things about

division in $R[x]$

PROPOSITION (11.2.9): For any ring R, if $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ is monic (i.e. leading coefficient $1 = a_n$)

then given any $g(x) \in R[x]$, one can find quotient $q(x) \in R[x]$

remainder $r(x) \in R[x]$

with $\deg(r(x)) < \deg(f(x))$

(CONVENTION: $\deg(0) = -\infty$)

such that $g(x) = q(x) \cdot f(x) + r(x)$.

Furthermore, $q(x), r(x)$ are unique.

$$\begin{array}{r} q(x) \\ f(x) \overline{)\, g(x)} \\ \vdots \\ \hline \vdots \\ \hline \vdots \\ \hline r(x) \end{array}$$

EXAMPLE: In $\mathbb{Z}/6\mathbb{Z}[x]$, $f(x) = x^2 - \bar{5}$, $g(x) = \bar{2}x^4 + x$

have $\bar{2}x^4 + x = (x^2 - \bar{5})(2\bar{x}^2 + \bar{4}) + (x + \bar{2})$

$g(x) = \underbrace{f(x)}_{\deg 2} \cdot g(x) + \underbrace{r(x)}_{\deg 1}$

$$\begin{array}{r} \bar{2}x^2 + \bar{4} = q(x) \\ x^2 - \bar{5} \overline{)\, \bar{2}x^4 + x = g(x)} \\ \bar{2}x^4 - \bar{10}x^2 \\ \hline \bar{4}x^2 + x \\ \bar{4}x^2 - \bar{20} \\ \hline x + \bar{2} = r(x) \end{array}$$

$f(x) = x^2 - \bar{5}$

proof: The existence of $q(x), r(x)$ given $f(x), g(x)$ comes from the usual division algorithm.

For uniqueness, if $g(x) = f(x)\,q_1(x) + r_1(x)$ with $\deg(r_1)$,
$= f(x)\,q_2(x) + r_2(x)$ $\deg(r_2) < \deg(f)$,

then $\underbrace{f(x)}_{\text{monic of some degree } d}(q_1(x) - q_2(x)) = \underbrace{r_2(x) - r_1(x)}_{\text{degree strictly less than } d}$

$$\Rightarrow \left\{ \begin{array}{l} q_1(x) - q_2(x) = 0 \\ r_2(x) - r_1(x) = 0 \end{array} \right\} \quad \text{i.e.} \quad \left\{ \begin{array}{l} q_1 = q_2 \\ r_1 = r_2 \end{array} \right\} \qquad \blacksquare$$

COROLLARY (11.2.10): The same holds when the leading coefficient of $f(x)$ lies in $R^\times$, and in particular for any $f(x) \neq 0$ when R is a field.

proof: If $f(x) = a_0 + a_1 x + \dots + a_n x^n$ and $a_n \in R^\times$

replace it by $a_n^{-1} f(x) = \frac{a_0}{a_n} + \frac{a_1}{a_n} x + \dots + \frac{a_{n-1}}{a_n} x^{n-1} + x^n$ which is monic,

then do $a_n^{-1} f(x) \overline{)\, g(x)}^{\,q(x)}$ (with remainder $r(x)$), and divide by a_n after. $\blacksquare$
q, r

NON-EXAMPLE: Can't divide everyone in $\mathbb{Z}[x]$ by $f(x) = 2x+1$ e.g. $g(x) = x^2$

The special case where $f(x) = x - \alpha$ relates to the substitution map $R[x] \longrightarrow R$: $x \longmapsto \alpha$

COROLLARY (11.2.11): The remainder when dividing $g(x) \in R[x]$ by $f(x) = x - \alpha$ for $\alpha \in R$ is the substitution $g(\alpha) \in R$

In particular, • $g(\alpha) = 0 \iff x - \alpha$ divides $g(x)$

• when R is a domain, $g(x) \neq 0$ can have at most $\deg(g)$ distinct roots $r_i \in R$ ($g(r_i) = 0$)

NOTE: False, for R not a domain e.g. $g(x) = \bar{2}x \in \mathbb{Z}/4\mathbb{Z}[x]$ has 2 distinct roots $x = \bar{0}$ but $\deg(g) = 1$

(and $g(x) = \bar{2}\cdot(x-\bar{0}) = \bar{2}(x-\bar{2})$)$^{x=\bar{2}}$