Exam 2 Total = 24

Average = 22.18
Median = 22
St. Dev = 4.85

NO CLASS THIS THURS Apr 10
HW 5 due Tues Apr 22
Exam 3 Thurs Apr 24.

We are studying polynomials in 1 variable over a field K.

Let $L \supseteq K$ be a field extension. Given $\alpha \in L$ we have an evaluation morphism

$$ev_\alpha : K[x] \to L$$
$$f(x) \mapsto f(\alpha).$$

Definition: We say that $\alpha \in L$ is algebraic over K if $\ker(ev_\alpha) \neq (0)$.

In this case since $K[x]$ is a PID we have

$$\ker(ev_\alpha) = (m_\alpha(x))$$

for some unique polynomial $m_\alpha(x) \in K[x]$ called the minimal polynomial of $\alpha \in L$ over K.

[We assume $m_\alpha(x)$ has leading coeff $= 1$.]

Last time we proved:

✡ Minimal Polynomial Theorem:

Let $\alpha \in L \supseteq K$ be algebraic with minimal polynomial $m_\alpha(x) \in K[x]$. Then

- $m_\alpha(x) \in K[x]$ is irreducible
- $K[\alpha] := \text{im}(\text{ev}_\alpha)$ is a subfield of L

Example: Consider $\sqrt{2} \in \mathbb{R} \supseteq \mathbb{Q}$. We know that

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

is a field because

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{(a-b\sqrt{2})}{(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2}$$

↓

$$= \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2}$$

$$\in \mathbb{Q}[\sqrt{2}].$$

We "rationalized the denominator".

Now consider $\sqrt[3]{2} \in \mathbb{R} \supseteq \mathbb{Q}$. The minpoly theorem says that

$$\mathbb{Q}[\sqrt[3]{2}] = \left\{ a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 : a, b, c \in \mathbb{Q} \right\}$$

is a field, but it is not obvious how to invert:

$$\frac{1}{a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)} = ? + ?\sqrt[3]{2} + ?\left(\sqrt[3]{2}\right)^2.$$

Observation: If $L \supseteq K$ is a field extension we can think of L as a <u>vector space</u> over K. Given $\alpha \in K$, $\beta \in L$, scalar multiplication is just multiplication

$$\alpha \cdot \beta := \alpha\beta. \text{ (Easy!)}$$

As such, we can consider the dimension of L as a K-vector space

$$[L:K] := \dim_K(L).$$

Theorem: If $\alpha \in L \supseteq K$ is algebraic with minpoly $m_\alpha(x) \in K[x]$ then

$$[K[\alpha]:K] = \deg(m_\alpha(x)).$$

Proof: Let $\deg(m_\alpha(x)) = n$. I claim that

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \in K[\alpha]$$

is a basis for $K[\alpha] \supseteq K$. There are two things to show.

(1) span?

Given any element $f(\alpha) \in K[\alpha]$ we divide $f(x)$ by $m_\alpha(x)$ in $K[x]$ to get

- $f(x) = q(x)m_\alpha(x) + r(x)$
- $r(x) = 0$ or $\deg(r) < \deg(m_\alpha)$.

Evaluate at α to get

$$f(\alpha) = q(\alpha)\, m_\alpha(\alpha) + r(\alpha)$$
$$= q(\alpha) \cdot 0 + r(\alpha)$$
$$= r(\alpha) \in \operatorname{span}_K \{1, \alpha, \ldots, \alpha^{n-1}\}.$$

(2) Independent?

Suppose we have

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0$$

for some $a_i \in K$ and let $f(x) := a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x]$. Note that $\deg(f) < n$. But since $f(\alpha) = 0$ we have

$$f(x) \in \ker(ev_\alpha) = (m_\alpha(x))$$

$$\Rightarrow m_\alpha(x) \mid f(x).$$

If $f(x) \neq 0$ this implies $n = \deg(m_\alpha) \leq \deg(f)$. Contradiction. Hence $f(x) = 0$, i.e.,

$$a_0 = a_1 = \cdots = a_{n-1} = 0.$$

Application to $\mathbb{Q}[\sqrt[3]{2}]$:

Let $\gamma := \sqrt[3]{2} \in \mathbb{R} \supseteq \mathbb{Q}$ and let $m_\gamma(x) \in \mathbb{Q}[x]$ be the minpoly.

Since $\gamma^3 - 2 = 0$ we have

$$x^3 - 2 \in \ker(ev_\gamma) = (m_\gamma(x))$$

$$\Longrightarrow \quad m_\gamma(x) \mid x^3 - 2$$

But I claim that $x^3 - 2$ is irreducible over $\mathbb{Q}$. If not, then we have

$$x^3 - 2 = f(x)\, g(x)$$

where one of $f, g \in \mathbb{Q}[x]$ has degree 1. WLOG suppose $f(x) = x - a \in \mathbb{Q}[x]$ so that

$$\begin{aligned} x^3 - 2 &= f(a)\, g(a) \\ &= (a - a)\, g(a) \\ &= 0 \end{aligned}$$

for some $a \in \mathbb{Q}$. Say $a = a/b$ with $a, b \in \mathbb{Z}$. Then we have

$$(a/b)^3 - 2 = 0$$
$$a^3 = 2b^3$$

This contradicts the fact that $\mathbb{Z}$ is UFD. Hence $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible and we conclude that

$$m_\gamma(x) = x^3 - 2.$$

Then $\mathbb{Q}[\gamma]$ is 3-dimensional with basis

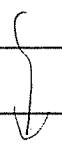
$$1, \gamma, \gamma^2.$$

We have

$$\mathbb{Q}[\gamma] = \{a + b\gamma + c\gamma^2 : a, b, c \in \mathbb{Q}\}.$$

To compute the inverse of a general element $a + b\gamma + c\gamma^2$ we want to solve for $x, y, z \in \mathbb{Q}$ in

$$(a + b\gamma + c\gamma^2)(x + y\gamma + z\gamma^2) = 1 + 0\gamma + 0\gamma^2.$$



Expand:

$$\begin{array}{lll} ax & +cy\gamma^3 + bz\gamma^3 & 1 \\ +bx\gamma & +ay\gamma + cz\gamma^4 & = +0\gamma \\ +cx\gamma^2 & +by\gamma^2 + az\gamma^2 & +0\gamma^2 \end{array}$$

$$\begin{array}{lll} ax & +2cy + 2bz & 1 \\ +bx\gamma & +ay\gamma + 2cz\gamma & = +0\gamma \\ +cx\gamma^2 & +by\gamma^2 + az\gamma^2 & +0\gamma^2 \end{array}$$

Equate coefficients to get a system of linear equations

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Solve using your favorite method to get

$$(a+b\gamma+c\gamma^2)^{-1}$$

$$= \left(\frac{a^2-2bc}{\Delta}\right) + \left(\frac{2c^2-ab}{\Delta}\right)\gamma + \left(\frac{b^2-ac}{\Delta}\right)\gamma^2$$

↓

where

$$\Delta = \det \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$$

$$= a^3 + 2b^3 + 4c^3 - 6abc .$$

Epilogue: we can still think of this as "rationalizing the denominator".

The so called "splitting field" of $x^3 - 2 \in \mathbb{Q}[x]$ is

$$\mathbb{Q}(\gamma, \omega) \supseteq \mathbb{Q}$$

where $\omega = e^{2\pi i/3}$. This field extension has a group of symmetries generated by

$$\varphi(\gamma) = \omega\gamma \quad \text{and} \quad \sigma(\gamma) = \gamma$$
$$\varphi(\omega) = \omega \qquad \sigma(\omega) = \overline{\omega}$$

This group called $\mathrm{Gal}(\mathbb{Q}(\gamma, \omega) \supseteq \mathbb{Q})$ is isomorphic to the dihedral group of order 6:

$$Gal = \{1, \varphi, \varphi^2, \sigma, \sigma\varphi, \sigma\varphi^2\}.$$

Given any element $\alpha \in \mathbb{Q}(\gamma, \omega)$ we regard the elements $g(\alpha) \in \mathbb{Q}(\gamma, \omega)$ for $g \in Gal$ as the "conjugates of α".

Finally, to "rationalize the denominator" we multiply the denominator by all of its conjugates

$$\frac{1}{\alpha} = \frac{1}{\alpha} \frac{\prod_{1 \neq g \in Gal} g(\alpha)}{\prod_{1 \neq g \in Gal} g(\alpha)} = \frac{\prod_{1 \neq g \in Gal} g(\alpha)}{\prod_{g \in Gal} g(\alpha)}.$$

The "rationalized" denominator

$$\prod_{g \in Gal} g(\alpha) \ni \mathbb{Q}$$

is called the "norm" of α. It is the same as the determinant we computed before.

4/15/14

HW 5 due Tues Apr 22
Exam 3 Thurs Apr 24
NO FINAL EXAM (for undergrads)

Recall: Last time we discussed the polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

It is irreducible over $\mathbb{Q}$ because it has no root in $\mathbb{Q}$

Proof: If $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is reducible then we have

$$f(x) = g(x)h(x)$$

where
- $g(x), h(x) \in \mathbb{Q}[x]$
- g, h are not units
  i.e. $\deg(g), \deg(h) > 0$
- g, h are not associate to f
  i.e. $\deg(g), \deg(h) < \deg(f)$.

Then since $3 = \deg(f) = \deg(g) + \deg(h)$, we conclude that

$$\deg(g) = 1 \quad \text{OR} \quad \deg(h) = 1.$$

WLOG assume $\deg(g) = 1$ so that

$$g(x) = \alpha x + \beta$$

for $\alpha, \beta \in \mathbb{Q}$ with $\alpha \neq 0$

But then $-\beta/\alpha \in \mathbb{Q}$ and

$$\begin{aligned} f(-\beta/\alpha) &= g(-\beta/\alpha)\, h(-\beta/\alpha) \\ &= (-\beta + \beta)\, h(-\beta/\alpha) \\ &= 0, \end{aligned}$$

hence $f(x)$ has a rational root $-\beta/\alpha$.

But if $-\beta/\alpha = a/b$ for $a, b \in \mathbb{Z}$ with $b \neq 0$ then

$$\left(\frac{a}{b}\right)^3 - 2 = 0$$

$$a^3 = 2b^3$$

Contradicts the fact that $\mathbb{Z}$ is a UFD.

Now let $m_{\sqrt[3]{2}}(x) \in \mathbb{Q}[x]$ be the minimal polynomial for $\sqrt[3]{2} \in \mathbb{R} \supseteq \mathbb{Q}$. Since

$$x^3 - 2 \in \ker\left(ev_{\sqrt[3]{2}} : \mathbb{Q}[x] \to \mathbb{R}\right)$$

we have $m_{\sqrt[3]{2}}(x) \mid x^3 - 2$ in $\mathbb{Q}[x]$

Then since $x^3 - 2$ is irreducible over $\mathbb{Q}$ we conclude that

$$m_{\sqrt[3]{2}}(x) = x^3 - 2$$

and hence $\mathbb{Q}[\sqrt[3]{2}]$ is a field which is 3-dimensional as a $\mathbb{Q}$-vector space with basis

$$1, \sqrt[3]{2}, (\sqrt[3]{2})^2.$$

That is,

$$\mathbb{Q}[\sqrt[3]{2}] = \left\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\right\}$$

with $a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2 = d + e(\sqrt[3]{2}) + f(\sqrt[3]{2})^2$

$$\Updownarrow$$

$a = d$, $b = e$, and $c = f$ in $\mathbb{Q}$.

Today: We can reverse this process.

Let K be a field and let $f(x) \in K[x]$ be an irreducible polynomial.

Then $f(x)$ has no roots in K.

[Recall Descartes: Given $\alpha \in K$ we have

$$f(\alpha) = 0 \iff f(x) = (x-\alpha)g(x)$$
for some $g(x) \in K[x]$.]

Q: Does $f(x)$ have a root in some field?

A: What do you mean by that?

Q: I mean, does there exist a field L containing a subfield $K' \leq L$ such that $K' \cong K$ and an element $\alpha \in L$ such that the homomorphism

$$ev_\alpha : K[x] \longrightarrow K'[x] \longrightarrow L$$

sends $f(x)$ to 0?

A: Oh, if you mean that then the answer is yes.

Proof: Define the quotient ring

$$L := K[x]/(f(x)).$$

Since $f(x)$ is irreducible and since $K[x]$ is a PID we conclude (see Exam 2) that $(f(x))$ is a maximal ideal, hence L is a field.

Furthermore, L has a subfield isomorphic to K. To see this think of $K \subseteq K[x]$ as the subring of constant polynomials and define a ring homomorphism

$$\varphi : K \longrightarrow K[x]/(f(x)) = L$$
$$a \longmapsto a + (f(x)).$$

This map is injective. Indeed given $a + (f(x)) = b + (f(x))$ for some $a, b \in K$ we have

$$a - b \in (f(x))$$

and hence $a-b = f(x)g(x)$ for some $g(x) \in K[x]$.
If $a-b \neq 0$ then

$$\deg(a-b) = \deg(f) + \deg(g)$$
$$\geq \deg(f) \geq 1.$$

This contradicts the fact that $a-b$ is a constant. Hence $a = b$. //

We conclude that $\ker \varphi = (0) \leq K$ and the First Isomorphism Theorem says

$$K = K/(0) \approx \operatorname{im} \varphi \subseteq L.$$

Hence $\operatorname{im} \varphi \subseteq L$ is a subfield isomorphic to K. Write $K' := \operatorname{im} \varphi$.

We can extend φ to a ring isomorphism

$$\varphi : K[x] \xrightarrow{\sim} K'[x] \subseteq L[x]$$

$$\sum_k a_k x^k \longmapsto \sum_k (a_k + (f(x)))\, x^k.$$

Finally, note that the polynomial $f(x) \in K[x]$ has a root in the field extension $L \supseteq K' \cong K$ (in a very silly and trivial way.)

Define $\alpha := x + (f(x)) \in L$. Then we have an evaluation homomorphism

$$ev_\alpha : K[x] \longrightarrow K'[x] \longrightarrow L$$

$$\sum a_k x^k \longmapsto \sum (a_k + (f(x)))x^k \mapsto \sum (a_k + (f(x)))(x + (f(x)))^k$$

and $\sum (a_k + (f(x)))(x + (f(x)))^k$

$$= \sum a_k x^k + (f(x)) \text{ by definition.}$$

Thus

$$ev_\alpha(f(x)) = f(x) + (f(x)) = 0 + (f(x)).$$

In other words:

$$f(\alpha) = 0.$$

We have found/contructed a field extension of K in which the irreducible $f(x) \in K[x]$ has a root.

But why stop there? In the field L Descartes' Theorem says that

$$f(x) = (x-\alpha)\,g(x) \quad \text{where}$$

- $g(x) \in L[x]$
- $\deg(g) = \deg(f) - 1$.

If $g(x)$ has no root in L we can repeat the process until we obtain a field

$$K \subseteq L \subseteq \cdots \subseteq S$$

and elements $\alpha_i \in S$ such that

$$f(x) = \prod_{i=1}^{\deg(f)} (x - \alpha_i) \in S[x].$$

[Note that the process will take $\leq \deg(f)$ steps to terminate.].

This S is called a <u>splitting field</u> for the polynomial $f(x) \in K[x]$.

To summarize, we have

"Kronecker's Theorem": Let K be a field and consider any nonzero, nonconstant polynomial. Then there exists a field extension $\delta \supseteq K$ in which $f(x)$ splits,

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

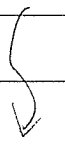
for some $\alpha_1, \ldots, \alpha_n \in \delta$.

Remark: If $f(x) \in \mathbb{Q}[x]$ then the Fundamental Theorem of Algebra says that $f(x)$ splits over $\mathbb{C}$.

But if K is some other field,

$$\text{say } K = \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

then we really do need Kronecker's Theorem.



Example: The polynomial

$$x^2 + 1 \in \mathbb{F}_7[x]$$

is irreducible over the field $\mathbb{F}_7$.

[Proof: If x^2+1 is reducible then it has a linear factor, hence it has a root in $\mathbb{F}_7$. But

$$\left.\begin{aligned} 1^2 &= 1 \neq -1 \\ 2^2 &= 4 \neq -1 \\ 3^2 &= 2 \neq -1 \\ 4^2 &= 2 \neq -1 \\ 5^6 &= 4 \neq -1 \\ 6^2 &= 1 \neq -1 \end{aligned}\right\} \text{ mod } 7$$

]

Hence there exists a field extension $L \supseteq \mathbb{F}_7$ and an element $\alpha \in L$ such that $\alpha^2 + 1 = 0$. Since x^2+1 is irreducible over $\mathbb{F}_7$ it is the minimal polynomial of α over $\mathbb{F}_7$:

$$m_\alpha(x) = x^2 + 1 \in \mathbb{F}_7[x].$$

$\S$

We conclude that $\mathbb{F}_7[\alpha] \subseteq L$ is a field which is 2-dimensional as a vector space over $\mathbb{F}_7$:

$$[\mathbb{F}_7[\alpha] : \mathbb{F}_7] = 2.$$

What is this mysterious field?

Since every element has a unique expression of the form $a + b\alpha$ with $a, b \in \mathbb{F}_7$ we have

$$|\mathbb{F}_7[\alpha]| = |\mathbb{F}_7|^2 = 7^2 = 49.$$

We just constructed a field of size 49. Maybe that's useful.

4/17/14

HW 5 due next Tues
Exam 3 next Thurs.
NO FINAL EXAM.

Last time we constructed a field of size 49.

Q: For which n does there exist a field of size n?

Let K be a field and assume that $|K| < \infty$. Consider the unique ring homomorphism

$$\varphi: \mathbb{Z} \longrightarrow K$$
$$1_{\mathbb{Z}} \longmapsto 1_K$$

Since $\operatorname{im}\varphi \subseteq K$ is a subring of a field it is a domain. Then since

$$\operatorname{im}\varphi \cong \mathbb{Z}/\ker\varphi$$

the kernel must be a prime ideal of $\mathbb{Z}$. That is,

$\ker\varphi = (0)$ or $\ker\varphi = (p)$ for some prime p.

Note that $\ker \varphi = (0)$ is impossible since then we would have

$$\operatorname{im}\varphi \cong \mathbb{Z}/(0) \cong \mathbb{Z}$$

and hence

$$\infty = |\operatorname{im}\varphi| \leq |K| < \infty.$$

Contradiction. Thus $\ker \varphi = (p)$ for some prime $p \in \mathbb{N}$, called the "characteristic" of the field K.

Furthermore, since prime $\Rightarrow$ maximal in a PID, the ideal $(p) < \mathbb{Z}$ is also maximal, so

$$\mathbb{Z}/(p) \cong \operatorname{im}\varphi < K.$$

is a subfield of K called the "prime subfield".

Notation: $\mathbb{F}_p := \mathbb{Z}/(p)$.

Thus we can think of K as a vector space over $\mathbb{F}_p$. Since $|K| < \infty$ it must be a finite dimensional vector space and hence

$$[K : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(K) = n.$$

For some $n \in \mathbb{N}$. We conclude that

$$|K| = |\mathbb{F}_p|^n = p^n.$$

Summary: Every finite field has size p^n for some $p, n \in \mathbb{N}$ with p prime.

Q: Does every size p^n occur?

Suppose there exists an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n.

Then by Kronecker's Theorem there exists a field $L \supseteq \mathbb{F}_p$ and an element $\alpha \in L$ such that

$$f(\alpha) = 0.$$

Since $f(x)$ is irreducible it is the minpoly

$$m_\alpha(x) = f(x) \in \mathbb{F}_p[x].$$

and hence $\mathbb{F}_p[\alpha]$ is a field which is n-dim over $\mathbb{F}_p$ with basis

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

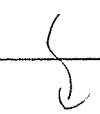
We conclude that

$$|\mathbb{F}_p[\alpha]| = |\mathbb{F}_p|^n = p^n.$$

Thus we have constructed a field of size p^n.

Example: $x^2 + 1 \in \mathbb{F}_7[x]$ is irreducible so there exists a field $\mathbb{F}_7[\alpha]$ of size $7^2 = 49$ where $\alpha^2 = -1 = 6 \in \mathbb{F}_7$

It is easy to do computations in this field. For example,



$$(2+5\alpha)(3+4\alpha)$$
$$= 6 + 15\alpha + 8\alpha + 20\alpha^2$$
$$= 6 + 23\alpha + 20 \cdot 6$$
$$= 21 \cdot 6 + 23\alpha$$
$$= 0 \cdot 6 + 2 \cdot \alpha$$
$$= 2\alpha.$$

You can think of this α as an "imaginary number" over $\mathbb{F}_7$ just like i is an imaginary number over $\mathbb{C}$.

///

Thus the question is:

Q: Do there exist irreducible polynomials of <u>every</u> degree in $\mathbb{F}_p[x]$?

Let $N_p(n) = \#$ irreducible $f(x) \in \mathbb{F}_p[x]$ with degree n and leading coeff. 1.

You will show on HW5 (following Gauss, 1889) that

$$\boxed{p^n = \sum_{d \mid n} d\, N_p(d)} \qquad (*)$$

Example: Fix prime $p \in \mathbb{N}$ and let $q \in \mathbb{N}$ also be prime. Then

$$p^q = \sum_{d \mid q} d N_p(d)$$
$$= 1 N_p(1) + q N_p(q).$$

But $N_p(1) = \#$ irreducible monic degree 1 polynomials $\in \mathbb{F}_p[x]$
$$= \#\{x - \alpha : \alpha \in \mathbb{F}_p\}.$$
$$= p.$$

Hence $p^q = p + q N_p(q)$.

$$\Rightarrow q N_p(q) = p^q - p$$
$$= p(p^{q-1} - 1) \neq 0.$$

$$\Rightarrow N_p(q) \neq 0.$$

Thus there exists an irreducible polynomial $\in \mathbb{F}_p[x]$ of degree q, and hence a field of size p^q.

↓

More generally, we have

$$p^{q^2} = \sum_{d \mid q^2} d\, N_p(d)$$

$$= 1 \cdot N_p(1) + q\, N_p(q) + q^2 N_p(q^2).$$

$$= p + (p^q - p) + q^2 N_p(q^2)$$

$$\Rightarrow q^2 N_p(q^2) = p^{q^2} - p^q$$

$$= p^q \left(p^{q(q-1)} - 1 \right) \neq 0$$

$$\Rightarrow N_p(q^2) \neq 0$$

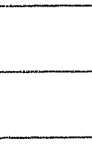
$$\Rightarrow \exists \text{ a field of size } p^{q^2}.$$

it's a bit tricky

By arguing similarly* we can show that for all $n \in \mathbb{N}$ we have

$$n N_p(n) = p^n + \sum_{i=0}^{n-1} a_i\, p^i$$

where a_i are some numbers $\in \{-1, 0, 1\}$



Hence

$$\sum_{i=0}^{n-1} a_i p^i \leq 1 + p + p^2 + \cdots + p^{n-1}$$

$$= \frac{(p^n - 1)}{(p-1)} < p^n - 1 < p^n.$$

We conclude that

$$n N_p(n) = p^n + \sum_{i=0}^{n-1} a_i p^i$$

$$> p^n - p^n = 0$$

$$\Longrightarrow N_p(n) > 0.$$

So there exists an irred. poly $\in \mathbb{F}_p[x]$ of degree n, and hence a field of size p^n.

Remark: That was not trivial, but it's good to know.

Q: How many (nonisomorphic) fields of size p^n are there?

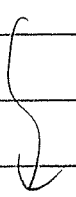
Every field of size p^n has the form

$$L := \mathbb{F}_p[x] / (f(x)) \supseteq \mathbb{F}_p$$

where $f(x) \in \mathbb{F}_p[x]$ is irreducible of degree n. (proof omitted). You will show that every element of L is a root of the polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$.

This implies that L is a "splitting field" for $x^{p^n} - x \in \mathbb{F}_p[x]$. (Certainly $x^{p^n} - x$ splits over L. But if $K \subsetneq L$ is any proper subfield then $x^{p^n} - x$ does not split over K because $x^{p^n} - x$ has no repeated roots and hence has p^n distinct roots, but $|K| < |L| = p^n$.)

Finally, we note that splitting fields are unique up to isomorphism. (proof omitted).



Summary: Let $p, n \in \mathbb{N}$ with p prime. We have seen that

- There exists a field of size p^n.
- Any two such fields are isomorphic.

Notation: This unique field is called

$$\mathbb{F}_{p^n}$$

and people often write $\mathbb{F}_q$ and assume that q is a prime power. An older notation says

$$\mathbb{F}_q = GF(q)$$

where GF stands for "Galois Field" because they were first studied by Galois ($\sim$1830).