Math 5402

4/15/20

Test 2 – Next weds.

Next Weds, no class.

You'll have a time window ($\geq$ 24hrs) and in that window you choose the 2hr period you want to take the test.

Window –

Weds morning – Thurs. night

I'll email you the test and post on website.

You take it and scan and email back to me.

<u>Theorem:</u> Let F either be a field of characteristic 0 (such as $\mathbb{Q}$) or a finite field.

Every irreducible polynomial over F is seperable.

A polynomial in $F[x]$ is seperable iff it is the product of distinct irreducible polynomials from $F[x]$.

[Corollary 34 / Prop 37 in the book]

<u>Theorem:</u> Let F be a field of characteric p where p is a prime. If $a, b \in F$, then

$$(a+b)^p = a^p + b^p$$

and $$(ab)^p = a^p b^p$$

Thus, the mapping $\varphi : F \to F$ given by $\varphi(x) = x^p$ is a field homomorphism.

Moreover, φ is injective (one-to-one)

(If F is finite, φ is onto.)

<u>Note:</u> If $f : S \to S$ is a function and S is finite then f is 1-1 iff f is onto.

proof: Let $a, b \in F$.

Then since F is commutative,

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots$$
$$\cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Note that $\binom{p}{i} \in \mathbb{Z}$ for $0 \leq i \leq p$,

so here we are thinking of

$\binom{p}{i}$ as $\underbrace{1 + 1 + \cdots + 1}_{\binom{p}{i} \text{ times}}$ where 1 is the 1 element of F.

Claim: $p \mid \binom{p}{i}$ if $1 \leq i \leq p-1$.

Why? Note that $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)!}{i!(p-i)!}$

and the numbers $(p-i)!$ and $i!$ only involve factors less than p (since $1 \leq i \leq p-1$). Hence the denominator cannot cancel the p in the numerator. [We are using that p is prime here.]

Since $p \mid \binom{p}{i}$ for $1 \le i \le p-1$
and F has characteristic p
we get that $\binom{p}{i} = 0$ for $1 \le i \le p-1$.
So, $(a+b)^p = a^p + b^p$.

Since F is commutative $(ab)^p = a^p b^p$.
So $\varphi : F \to F$ given by
$\varphi(x) = x^p$ is a field homomorphism.

Let's show φ is one-to-one.

We Know $\operatorname{Ker}(\varphi)$ is an ideal
of F. Since F is a field,
$\ker(\varphi) = \{0\}$ or $\ker(\varphi) = F$.
But $\varphi(1) = 1^p = 1 \neq 0$.
So, $1 \notin \ker(\varphi)$. So, $\ker(\varphi) \neq F$.
Thus, $\ker(\varphi) = \{0\}$ and
φ is 1-1. $\blacksquare$

The function $\varphi : F \to F$ given by $\varphi(X) = X^p$ is called the <u>Frobenius endomorphism on F</u>. (Here $\text{char}(F) = p$)

<u>Thm:</u> Let p be a prime and $n \in \mathbb{Z}$, $n \geq 1$. There exists a finite field $\mathbb{F}_{p^n}$ of size p^n.

<u>proof:</u> Let $\mathbb{F}_{p^n}$ be a splitting field for $X^{p^n} - X$ over $\mathbb{Z}_p$. Last time we saw that this polynomial is seperable and hence has no multiple roots in $\mathbb{F}_{p^n}$. So, $X^{p^n} - X$ has precisely p^n roots in $\mathbb{F}_{p^n}$.

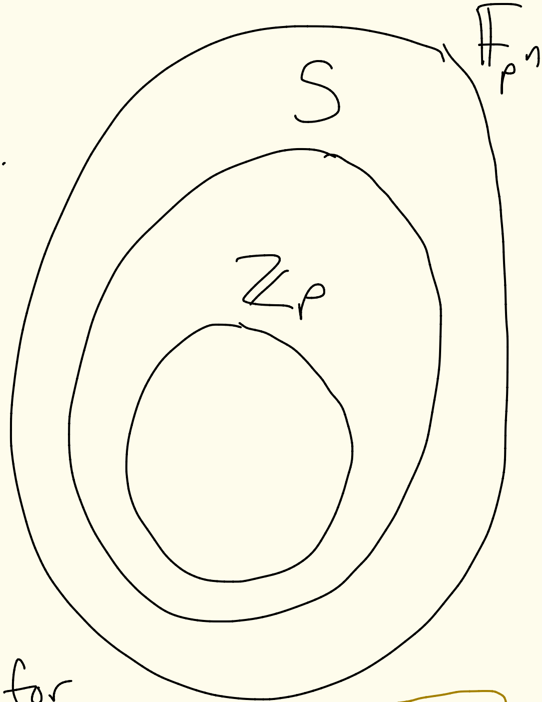
Let $S = \{\alpha \in \mathbb{F}_{p^n} \mid \alpha^{p^n} - \alpha = 0\}$.

So, $|S| = p^n$.

Note that $\mathbb{Z}_p \subseteq S$.

Why? If $x \in \mathbb{Z}_p^\times$, then $x^{p-1} - 1 = 0$. (since $\mathbb{Z}_p^\times$ is a group of size $p-1$ under multiplication).

So, $x^p - x = 0$ or $x^p = x$.



This is also true for $x = 0$. Thus, $\boxed{x^p = x \text{ for all } x \in \mathbb{Z}_p.}$

Thus, $x^{p^n} = x^{p \cdot p \cdots p} = (((x^p)^p)\cdots)^p = x, \ \forall x \in \mathbb{Z}_p$.

So, $x^{p^n} - x = 0 \quad \forall x \in \mathbb{Z}_p$.

Thus, $\mathbb{Z}_p \subseteq S \subseteq \mathbb{F}_{p^n}$.

Let's show $S = \mathbb{F}_{p^n}$. pg 8

Let $\alpha, \beta \in S$. Then $\alpha^{p^n} = \alpha$
and $\beta^{p^n} = \beta$.

So, $(-\beta^{p^n}) = (-1)^{p^n} \beta^{p^n} = -\beta$ ← If $p=2$, $-1=1$

① $0^{p^n} = 0$, $1^{p^n} = 1$, so $0 \in S$, $1 \in S$.

② $(\alpha - \beta)^{p^n} = \alpha^{p^n} + (-\beta)^{p^n} = \alpha - \beta$

repeated use of Frobenius automorphism

$$(a+b)^p = a^p + b^p$$

ex: $(a+b)^{p^2} = ((a+b)^p)^p = (a^p + b^p)^p$
$= (a^p)^p + (b^p)^p = a^{p^2} + b^{p^2}$

So, $\alpha - \beta \in S$

③ $(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta$. So, $\alpha\beta \in S$.

④ $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. So, $\alpha^{-1} \in S$.

By ①, ②, ③, ④ we have that
S is a subfield of $\mathbb{F}_{p^n}$.

So, S is a field containing all the roots of $x^{p^n} - x = 0$.
So, S itself is a splitting field of $x^{p^n} - x$. So, $\mathbb{F}_{p^n} = S$.
And $|\mathbb{F}_{p^n}| = p^n$. $\boxed{/\!/}$

<u>Theorem:</u> If F is a finite field then $|F| = p^n$ where p is prime. All other finite fields of size p^n are isomorphic to F.

<u>proof:</u> Let F be a finite field of characteristic p where p is prime. Consider the prime subfield

$$\mathbb{Z}_p \cong \{0, 1, 1+1, 1+1+1, \dots, \underbrace{1+\dots+1}_{p-1 \text{ times}}\}$$

So, F is an extension of $\mathbb{Z}_p$.

Suppose $[F:\mathbb{Z}_p]=n$

$[F:\mathbb{Z}_p]$ must be finite since F is finite

So,

$$F=\{a_1\beta_1+a_2\beta_2+\cdots+a_n\beta_n \mid a_i\in\mathbb{Z}_p\}$$

where $\{\beta_1,\ldots,\beta_n\}$ is a basis for F over $\mathbb{Z}_p$.

Thus, $|F| = \underbrace{p}_{\text{choices for } a_1}\cdot\underbrace{p}_{\text{choices for } a_2}\cdot\cdots\cdot\underbrace{p}_{\text{choices for } a_n}=p^n$.

Since $F^\times=F-\{0\}$ is a group under multiplication of size p^n-1, we get that $\alpha^{p^n-1}=1$ $\forall\alpha\in F^\times$. So, $\alpha^{p^n}-\alpha=0$ for all $\alpha\in F^\times$. Also, $0^{p^n}-0=0$. So, $\alpha^{p^n}-\alpha=0$ for all $\alpha\in F$.

pg 11

Since $|F| = p^n$ and

$\alpha^{p^n} - \alpha = 0 \quad \forall \alpha \in F$

we get that F is a splitting field for $X^{p^n} - X$.

So, $F \cong \mathbb{F}_{p^n}$ since splitting fields are isomorphic. $\blacksquare$