2/29/16

Lecture 18 Monday Feb 29

COR 15 In the group $\mathbb{Z}_N^\times$ the equation

$$x^p = 1$$

has exactly p solutions

$$1, \quad 1+p^{n-1}, \quad 1+2p^{n-1}, \quad \ldots, \quad 1+(p-1)p^{n-1}$$

pf Set $t = n-1$ in LEM 14 and recall $N = p^n$ $\square$

LEM 16 The group B is cyclic.

pf Recall

$$B = \{ b \in \mathbb{Z}_N^\times \mid b^{p^{n-1}} = 1 \}$$

$$|B| = p^{n-1}$$

For $0 \le i \le n-1$ define

$$B_i = \{ b \in \mathbb{Z}_N^\times \mid b^{p^i} = 1 \}$$

So

$$1 = B_0 \le B_1 \le B_2 \le \cdots \le B_{n-1} = B$$

Obs

$$b \in B \implies b^p \in B$$

Consider the map

$$\sigma : \begin{array}{ccc} B & \to & B \\ b & \to & b^p \end{array}$$

By Cor 15, for $\theta \in B$ the set

$$\{ b \in B \mid \sigma(b) = \theta \}$$

is either empty or has exactly p elements.

So σ is "p to 1"

By constr

$$\sigma(B_i) \subseteq B_{i-1} \qquad 1 \le i \le n-1$$

So

$$|B_i| \le p\,|B_{i-1}| \qquad 1 \le i \le n-1$$

So

$$|B_i| \le p^i \qquad 0 \le i \le n-1$$

Now

$$|B_{n-2}| \le p^{n-2} < p^{n-1} = |B_{n-1}|$$

So

$$B_{n-2} \subsetneq B_{n-1} = B$$

$\exists$

$$\theta \in B \setminus B_{n-2}$$

By const θ has order p^{n-1}

so θ generates B

So B is cyclic. $\square$

Prop 17 For $N = p^n$, odd prime p, $n \geq 1$

the group $\mathbb{Z}_N^\times$ is cyclic.

pf For $n=1$ this is Ex 6

Assume $n \geq 2$

Recall the groups A, B are cyclic.

Also $|A| = p-1$ $|B| = p^{n-1}$

rel prime

So $A \times B$ is cyclic by CH REM THM.

We saw

$\mathbb{Z}_N^\times$ iso $A \times B$

So $\mathbb{Z}_N^\times$ is cyclic. $\square$

Chapter 10 Modules

Before defining a module we give some motivations

<u>Motivation I</u> Given an abelian group $M, +, 0$

Recall

$$a+b = b+a$$

$$a+0 = 0+a = a$$

$$(a+b)+c = a+(b+c)$$

$\forall a \; \exists b$ st write $b=-a$

$$a+b = b+a = 0$$

$\forall a \in M$ write

$$\cdots$$

$$3a = a+a+a$$

$$2a = a+a$$

$$1a = a$$

$$0a = 0$$

$$(-1)a = -a$$

$$(-2)a = -a-a$$

$$\cdots$$

This defines na for $n \in \mathbb{Z}$ and $a \in M$.

The map

$$\mathbb{Z} \times M \longrightarrow M$$
$$n \quad a \longrightarrow na$$

satisfies

$(r+s)a = ra + sa$ $\qquad r, s \in \mathbb{Z} \quad a \in M$

$(rs)a = r(sa)$ $\qquad$ ..

$r(a+b) = ra + rb$ $\qquad r \in \mathbb{Z} \quad a, b \in M$

$1a = a$ $\qquad a \in M$

Motivation II   Let F = field

Pick integer $n \geq 1$

Let V = vector space over F consisting of the row vectors

$(\alpha_1, \alpha_2, \ldots, \alpha_n)$ $\alpha_i \in F$ $1 \leq i \leq n$

Recall $V, +$ is an abelian group with identity

$0 = (0, 0, \ldots, 0)$

View scalar mult as a function

$$F \times V \to V$$

$$\alpha \quad v \to \alpha v$$

that satisfies

$(\alpha + \beta) v = \alpha v + \beta v$ $\alpha, \beta \in F$ $v \in V$

$(\alpha \beta) v = \alpha(\beta v)$ "

$\alpha(u + v) = \alpha u + \alpha v$ $\alpha \in F$ $u, v \in V$

$1 v = v$ $v \in V$

Motivation III Let the field F and vector space V as above.

Fix a linear transformation $T: V \to V$

Recall $T^2: V \to V$ is the composition

$$T^2: V \xrightarrow{T} V \xrightarrow{T} V$$

Similarly $T^3: V \xrightarrow{T} V \xrightarrow{T} V \xrightarrow{T} V$

etc

View $T^0 = I$ (identity map on V)

$T^n: V \to V$ is a linear trans for $n = 0, 1, 2, \ldots$

Let x = indet

Consider polynomial ring $F[x]$

For $f(x) \in F[x]$ write

$$f = c_0 + c_1 x + \cdots + c_\ell x^\ell \qquad c_i \in F$$

The map

$$f(T) : V \longrightarrow V$$
$$v \longrightarrow c_0 v + c_1 T v + \cdots + c_n T^n v$$

is a linear trans

The map

$$F[x] \times V \longrightarrow V$$
$$f(x) \quad v \longrightarrow f(T) v$$

satisfies

$$(r+s)v = rv + sv \qquad r, s \in F[x] \quad v \in V$$

$$(rs)v = r(sv)$$

$$r(u+v) = ru + rv \qquad r \in F[x] \quad u, v \in V$$

$$1v = v \qquad v \in V$$

We now define a module

Def 1 Given a ring R (not nec commutative), an <u>R-module</u> is an abelian group $M, +, 0$ together with a map

$$R \times M \to M$$
$$r \quad a \to ra$$

such that

$$(r+s)a = ra + sa \qquad r, s \in R \quad a \in M$$

$$(rs)a = r(sa) \qquad \text{"} \quad \text{"}$$

$$r(a+b) = ra + rb \qquad r \in R, \quad a, b \in M$$

If R has 1 the we also require

$$1a = a \qquad a \in M$$

Note Above R-module is sometimes called a left R-module.
A right R-module is similarly defined with action

$$M \times R \to R$$
$$a \quad r \to ar$$

DEF 2 Given an R-module M

An <u>R-submodule</u> of M is a subgroup N of M

such that $ra \in N$ $\forall r \in R$ $\forall a \in N$.

Ex 3 (i) A $\mathbb{Z}$-module is essentially the same thing as an abelian group. The $\mathbb{Z}$-submodules correspond to the subgroups.

(ii) For a field F, an F-module is essentially the same thing as a vector space over F. The F-submodules correspond to the subspaces

(iii) For a field F and an indet x, an $F[x]$-module is essentially the same thing as a vector space V over F, together with a fixed lin trans $T : V \to V$. The $F[x]$-submodules of V correspond to the subspaces W of V such that

$T(w) \in W \quad \forall w \in W$ "T-stable subspaces" "T-invariant subspaces"

Until further notice R is any ring

Ex 4 $M = R$ is an R-module with action

$$R \times M \to M$$
$$r \quad a \mapsto \underset{\substack{\uparrow \\ \text{mult in } R}}{ra}$$

An R-submodule of M is the same thing as a left ideal of R

Ex 5 Given an R-module M

Define

$$I = \{ r \in R \mid ra = 0 \ \forall a \in M \}$$

"annihilator of M"

then I is a 2-sided ideal of R

Ex 6 Given R-module M

Given a 2-sided ideal $I \triangleleft R$ st

$ra = 0$ for $r \in R$ and $a \in M$.

then M becomes a (R/I)-module

with action

$$\begin{aligned} R/I \times M &\to M \\ r+I \quad a &\mapsto ra \end{aligned}$$