# MIDTERM overview

3/14/11

1) (b) Show $U(15)$ is not cyclic.

$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Assume by contradiction that $U(15)$ is cyclic.

$U(15) \cong \mathbb{Z}_8$

But $\{4, 11, 14\} \in U(15)$

$4 \cdot 4 = 16 = 1 \bmod(15) = 11 \cdot 11 = 14 \cdot 14$

But $\mathbb{Z}_8$ has only 1 element of order 2, $n=4$.

2) $[G:H] = 2 \Rightarrow$ 2 left cosets
2 right cosets

left coset: $H, gH \Rightarrow g_1H = GH$

right: $H, Hg_1 \Rightarrow Hg_1 = GH$

$\Rightarrow Hg_1 = g_1H \; \forall \; g_1 \in H$

3) consider $T \subseteq S$

$\sigma \in S_{n+m}$, $\sigma = ab \Rightarrow a$ is the product of cycles which permute $\{1, 2 \dots n\}$, $b$ is the product of cycles which permute $\{n+1, n+2 \dots n+m\}$

$\sigma = ab \Rightarrow (a, \hat{b})$, $\hat{b}$ permutes $\{1, 2 \dots m\}$

4) $A = \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}$ $B = \begin{bmatrix} 2 & 2 \\ -2 & 2 \end{bmatrix}$

$A^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $B^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$A+B = \begin{bmatrix} 1 & 3 \\ -3 & -1 \end{bmatrix}$, $(A+B)^2 = \begin{bmatrix} -8 & 0 \\ 0 & -8 \end{bmatrix}$

5) No, ex: $G = \mathbb{Z}_6$ $H = \mathbb{Z}_4$

$\varphi(e_0) = e$ $\varphi(0) = 0$

$\varphi: G \to H$ $\varphi(1) = 3$ $\varphi(2) = 1$

$\varphi(3) = 2$ $\varphi(4) = 3$ $\varphi(5) = 1$

# Rings Chapter 17

**Def:** A ring $R$ is a set with two binary operations $(+, \cdot)$ such that:

a) $(R, +)$ is an abelian group.
("+" is some commutative operation on $R$)

b) $\forall x, y, z \in R$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(associativity under "$\cdot$")

c) $\forall x, y, z \in R$, $x \cdot (y + z) = x \cdot y + x \cdot z$
$(x + y) \cdot z = x \cdot z + y \cdot z$
(distributivity of "$\cdot$" over "$+$")

## Further Definitions

1) $R$ is commutative if $x \cdot y = y \cdot x \quad \forall x, y \in R$
2) $R$ has a unit for "$\cdot$" if $\exists z \in R \ni$
$z \cdot x = x \cdot z = x \quad \forall x \in R$
we usually write $z = 1_R$ (or just "1")
The additive identity is denoted by $0_R$ (or just "0")

## Examples

1) $R = \mathbb{Z}$ "$+$" is regular addition
"$\cdot$" is regular multiplication.
unit = 1
$\mathbb{Z}$ is a commutative ring

2) $R = \mathbb{Z}_n$ is also a ring
"$+$" = addition mod $n$
"$\cdot$" = multiplication mod $n$.
unit = 1
$\mathbb{Z}_n$ is a commutative ring.

3) $M_n(\mathbb{R})$ (or $M_n(\mathbb{C})$) is a ring.

"+" = matrix addition

"·" = matrix multiplication

unit = $n \times n$ identity matrix $= \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$M_n(\mathbb{R})$ or $M_n(\mathbb{C})$ are not commutative rings.

4) $R = \{$polynomials with integer coefficients$\}$

"+" = polynomial addition

suppose $p(x) = \sum_{i=0}^{n} a_i x^i$

$q(x) = \sum_{j=0}^{m} b_j x^j$ where $a_i, b_j \in \mathbb{Z}$ for $0 \le i \le n$, $0 \le j \le m$

suppose $n \ge m$

$p(x) + q(x) = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i$

$p(x) = x^2 + 5$

$q(x) = -9x^3 + 2x^2 + 3x + 1$

$p(x) + q(x) = -9x^3 + (2+1)x^2 + 3(x) + (5+1)$

$= -9x^3 + 3x^2 + 3x + 6$

"·" = polynomial multiplication

$p(x) \cdot q(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j}$

$p(x) = x^2 + 5$

$q(x) = -9x^3 + 2x^2 + 3x + 1$

$p(x) \cdot q(x) = x^2(-9x^3 + 2x^2 + 3x + 1) + 5(-9x^3 + 2x^2 + 3x + 1)$

$= -9x^5 + 2x^4 + 3x^3 + x^2 - 45x^3 + 10x^2 + 15x + 5$

$= -9x^5 + 2x^4 - 42x^3 + 11x^2 + 15x + 5$

Note: "+" and "·" are binary operations since $\mathbb{Z}$ is a ring.

unit = 1

commutative? yes.