3/9/11

Last time:

$|G| < \infty$, $H \leq G$

$[G:H] = \#$ of left cosets

left cosets:

$|gH| = |H|$

$G = \bigcup_{i=1}^{n} g_i H$

$|G| = n|H| \Rightarrow n = [G:H]$

Recall:

$H \trianglelefteq G$, then a group structure on the left cosets of H in G is given by $(g, k \in G)$

$gH * kH = (gk)H$

With this binary operation, the left cosets form a group.

Thm: (First Isomorphism Theorem $\Downarrow$ or "Fundamental Homomorphism Theorem")

- let G, H be groups and $\varphi: G \to H$ be a homomorphism. Then $\varphi(G) \cong \{$left cosets of $\mathrm{Ker}(\varphi)\}$

(Notation for left cosets: $G/\ker\varphi$)

Pf: $\varphi(G)$ is a subgroup of H since if $g \in G$, $\varphi(g)^{-1} = \varphi(g^{-1}) \in \varphi(G)$ and if $k \in G$, $\varphi(g)\varphi(k) = \varphi(gk) \in \varphi(G)$ (two step subgroup test)

$\varphi(G) \neq \emptyset$ since $\varphi(e_G) = e_H \in \varphi(G)$

Construct an isomorphism btw $G/\ker\varphi$ and $\varphi(G)$

Define $\psi: G/\ker\varphi \to \varphi(G)$ as for $g \in G$

$\psi(g\ker\varphi) = \varphi(g)$, ψ is surjective by definition

check: 1) ψ is injective

2) ψ is a homomorphism

3) ψ is well-defined (if $g\ker\varphi = t\ker\varphi$, then $\psi(g\ker\varphi) = \psi(t\ker\varphi)$)

Pf con't: 1) Injectivity:

Suppose $g, t \in G$ and $\Psi(g\ker\varphi) = \Psi(t\ker\varphi)$. Then $\varphi(g) = \varphi(t)$. We have as a consequence that $\varphi(t)^{-1}\varphi(g) = e_H$. φ is a homomorphism, so $\varphi(t)^{-1}\varphi(g) = \varphi(t^{-1})\varphi(g) = \varphi(t^{-1}g)$.

$\ker\varphi = \{g \in G : \varphi(g) = e_H\}$ $\rightarrow$ this says that $\varphi(t^{-1}g) \in e_H$, so $t^{-1}g \in \ker\varphi$. By lemma from last time, $t^{-1}g \in \ker\varphi$ iff $t\ker\varphi = g\ker\varphi$, so Ψ is injective

2) Homomorphism:

take $g, t \in G$. $\Psi(g\ker\varphi)\Psi(t\ker\varphi)$
$= \varphi(g)\varphi(t) = \varphi(gt)$
$= \Psi(gt\ker\varphi) = \Psi(g\ker\varphi * t\ker\varphi)$ ✓

3) well-defined:

Suppose $g, t \in G$ and $g\ker\varphi = t\ker\varphi$. By lemma from last class, $t^{-1}g \in \ker\varphi$.
This implies $e_H = \varphi(t^{-1}g) = \varphi(t^{-1})\varphi(g)$
$= \varphi(t)^{-1}\varphi(g)$
so, $\varphi(t) = \varphi(g)$
but, $\varphi(t) = \Psi(t\ker\varphi)$ and $\varphi(g) = \Psi(g\ker\varphi)$
so, $\Psi(t\ker\varphi) = \Psi(g\ker\varphi)$.

Notation:

If $H \trianglelefteq G$, then G/H denotes the left cosets of H in G with the group structure $(g, k \in G)$ $(gH) * (kH) = (gk)H$. called a quotient or factor group.

Examples

1) $G = \mathbb{Z}$, $H_n = \{n \cdot k : k \in \mathbb{Z}\}$
$\mathbb{Z}$ abelian implies $H_n \trianglelefteq G$.
What is the isomorphism class of $\mathbb{Z}/H_n$?

We showed before the midterm that $[\mathbb{Z} : H_n] = n$
Claim: $\mathbb{Z}/H_n \cong \mathbb{Z}_n$
Define $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ by $\varphi(k) = k \pmod n$
you can check if $k, m \in \mathbb{Z}$, then
$(km) \bmod n = (k \bmod n \circ m \bmod n) \bmod n$
This shows φ is a homomorphism.
$\ker\varphi = \{k \in \mathbb{Z} \mid \varphi(k) = 0 \pmod n\}$
$= \{k \in \mathbb{Z} \mid k = nm \text{ for } m \in \mathbb{Z}\} = H_n$
φ is surjective since if $0 \leq k \leq n-1$, $\varphi(k) = k$
By the first isomorphism thm, $\mathbb{Z}/H_n \cong \mathbb{Z}_n$
(sometimes people write $H_n = n\mathbb{Z}$, then the isomorphism is $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$)

2) $G = S_n$, $H = A_n = \{\sigma \in S_n : \sigma \text{ is even}\}$
Claim: $S_n/A_n \cong \mathbb{Z}_2$
Define $\varphi_n : S_n \to \mathbb{Z}_2$, $\varphi_n(\sigma) = \begin{cases} 0, & \sigma \text{ even} \\ 1, & \sigma \text{ odd} \end{cases}$

φ_n is surjective and $\ker(\varphi_n) = A_n$.
φ_n is a homomorphism since, even $\cdot$ even = even, odd $\cdot$ even = odd, and odd $\cdot$ odd = even.
For ex: If $\sigma_1, \sigma_2 \in S_n$ and σ_1 is odd, σ_2 is odd,
$\varphi(\sigma_1) + \varphi(\sigma_2) = 1 + 1 = 0 \bmod 2$
$\sigma_1\sigma_2$ is even, so $\varphi(\sigma_1\sigma_2) = 0$
By the first isomorphism thm, $S_n/A_n \cong \mathbb{Z}_2$
(Corollary: $|A_n| = \frac{n!}{2}$)

cont
Ex from last class

Examples with Rings

3/16/11

Back to polynomials:

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

(Notation: $\mathbb{Z}[x]$)

$p(x) = \sum_{i=0}^{n} \alpha_i x^i \qquad q(x) = \sum_{j=0}^{m} \beta_j x^j$

α_i's β_j's are integers

suppose $n \geq m$

$(p+q)(x) = \sum_{i=0}^{m} (\alpha_i + \beta_i) x^i) + \sum_{i=m+1}^{n} \alpha_i x^i$.

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

show for $p, q, r \in \mathbb{Z}[x]$

$(p \cdot q) \cdot r = p \cdot (q \cdot r)$ (associativity)

$p(x) = \sum_{i=0}^{n} \alpha_i x^i, \quad q(x) = \sum_{j=0}^{m} \beta_j x^j, \quad r(x) = \sum_{k=0}^{l} \gamma_k x^k$

α_i's, β_j's, γ_k's are integers

$p \cdot (q \cdot r)(x)$

$(q \cdot r) = \sum_{j=0}^{m} \sum_{k=0}^{l} \beta_j \gamma_k x^{j+k}$

$p \cdot (q \cdot r) = \sum_{i=0}^{n} \sum_{j=0}^{m} \sum_{k=0}^{l} \alpha_i (\beta_j \gamma_k) x^{i+(j+k)}$

$(p \cdot q) \cdot r(x)$

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

$(p \cdot q) \cdot r(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} \sum_{k=0}^{l} (\alpha_i \beta_j) \gamma_k x^{(i+j)+k}$

$(\alpha_i \beta_j) \gamma_k = \alpha_i (\beta_j \gamma_k)$ and $(i+j)+k = i+(j+k)$ by associativity of multiplication and addition on $\mathbb{Z}$. Therefore, $p \cdot (q \cdot r) = (p \cdot q) \cdot r$

Examples

1) $R = C_0(\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ is cont } + \lim_{|x|\to\infty} f(x) = 0 \}$

"continuous functions vanishing at infinity"

"+" $(f+g)(x) = f(x) + g(x)$

"·" $(f \cdot g)(x) = f(x) \cdot g(x)$

Associativity of "·" and distributivity follow from associativity and distributivity of regular multiplication and addition on $\mathbb{R}$.

e.g.:

$f, g, h \in C_0(\mathbb{R})$

$$f \cdot (g+h)(x) = f(x) \cdot (g+h)(x) = f(x)(g(x) + h(x))$$
$$= f(x) \cdot g(x) + f(x) \cdot h(x)$$
$$= (f \cdot g)(x) + (f \cdot h)(x)$$

distributivity in one direction

$C_0(\mathbb{R}) \neq \emptyset$ since $0 \in C_0(\mathbb{R})$.

$C_0(\mathbb{R})$ is a ring.

Commutative since regular multiplication of real numbers is commutative

✓ $(f \cdot g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x)$ (real # comm)
$= (g \cdot f)(x)$

If $C_0(\mathbb{R})$ had a unit, it would have to be $f(x) \equiv 1$ but $1 \notin C_0(\mathbb{R})$ since $\lim_{|x|\to\infty} 1 \neq 0$

So, $C_0(\mathbb{R})$ has no unit

2) $R = \{T \in M_2(\mathbb{R}) \mid T$ has even integer entries$\}$

$T = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ such that $a_{ij} \in \mathbb{Z}$ and a_{ij} is even $\forall\, i,j$.

"$+$" = matrix addition

"$\cdot$" = matrix multiplication

Associativity and distributivity follow from associativity and distributivity on $M_2(\mathbb{R})$.

Is $\langle R, + \rangle$ an abelian group?

let $S, T \in R$

Identity of $\langle R,+\rangle \doteq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$ since 0 even

Inverse of S in $\langle R,+\rangle = -S \in R$

since if a_{ij} is even, $-a_{ij}$ is also even

Closure:

let $T = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ $S = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$

a_{ij}'s b_{ij}'s are even integers

$$S+T = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$
$$= \begin{pmatrix} b_{11}+a_{11} & b_{12}+a_{12} \\ b_{21}+a_{21} & b_{22}+a_{22} \end{pmatrix} = T+S$$

So "$+$" is commutative and $T+S \in R$ since the sum of even numbers is even

so, $\langle R,+\rangle$ is an abelian group

Is "$\cdot$" a binary operation on R

i.e. if $S, T \in R$ is $S \cdot T \in R$?

$$S \cdot T = \begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix}$$

the product of even integers is even and we've already noted the sum is even so, $S \cdot T \in R$

e.g. $T = \begin{pmatrix} 2 & 6 \\ 4 & 8 \end{pmatrix}$ $S = \begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix}$

$S \cdot T = \begin{pmatrix} 4 & 12 \\ 40 & 80 \end{pmatrix} \in R$ →

Is "$\cdot$" a commutative operation on R? NO

$T = \begin{pmatrix} 2 & 6 \\ 4 & 8 \end{pmatrix}$ $S = \begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix}$

$ST = \begin{pmatrix} 4 & 12 \\ 40 & 80 \end{pmatrix} \neq TS = \begin{pmatrix} 4 & 60 \\ 8 & 80 \end{pmatrix}$

Is there a unit?

If there were a unit, it would be $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ but $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin R$ since 1 is odd, so R has no unit

Def: $S \subseteq R$, R is a ring. S is a subring of R if $S \neq \emptyset$ and S is a ring with the same operations as R.

Warning: If R has a unit, S could have a different unit from R. I $1_R \in S$, then we say S is unital.

Examples of Subrings

1) $R = M_2(\mathbb{R})$ with matrix multiplication + addition

$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \ a \in \mathbb{R} \right\}$

Then S is a subring of R but $1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$

S does have an identity!

$1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in S$