Quiz Friday on lectures 18–24

10/29/2018

Last time – Discussed 3 Sylow theorems.

– Used them to prove: if G is a group with $|G| = pq$, p, q primes, $q < p$, then

(i) $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$ if $q \nmid (p-1)$

(ii) $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$ if $q \mid (p-1)$

Unfinished business: p prime

$\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times = \{[1], \ldots [p-1]\}$ = the group of units of $\mathbb{Z}_p$.

Proof For any $f \in \mathrm{Aut}(\mathbb{Z}_p)$, $f([k]) = [k]\, f([1])$

Hence, since f is not zero, $f([1]) \neq [0]$ in $\mathbb{Z}_p$.

$\Rightarrow f([1]) \in \mathbb{Z}_p^\times$.

We get a map $\Psi : \mathrm{Aut}(\mathbb{Z}_p) \to \mathbb{Z}_p^\times$, $\Psi(f) = f([1])$.

We now argue that Ψ is an isomorphism.

$\Psi(f \circ g) = (f \circ g)([1]) = f(g[1]) = (g[1]) \cdot f([1])$

↑ since $f([k]) = [k]\, f([1])$ $\forall [k] \in \mathbb{Z}_p$

$= \Psi(g) \cdot \Psi(f) = \Psi(f) \cdot \Psi(g)$ (since $\circ$ is commutative)

If $\Psi(f) = [1]$, $f([1]) = [1] \Rightarrow f([k]) = [k][1] = [k]$ $\forall [k] \in \mathbb{Z}_p$

$\Rightarrow f = \mathrm{id}_{\mathbb{Z}_p}$. $\Rightarrow \ker \Psi = \{\mathrm{id}_{\mathbb{Z}_p}\}$

$\Rightarrow \Psi$ is 1–1.

Given $[a] \in \mathbb{Z}_p^\times$, the map $h : \mathbb{Z}_p \to \mathbb{Z}_p$, $h([k]) := [k][a]$ is a homomorphism since $([k] + [\ell])[a] = [k][a] + [\ell][a]$

Moreover h has an inverse: $h^{-1}([k]) = [k][a]^{-1}$.

$\Rightarrow h$ is an isomorphism.

Finally $h([1]) = [1][a] = [a]$.

$\Rightarrow$ $\forall [a] \in \mathbb{Z}_p^\times$ $\exists h \in \mathrm{Aut}(\mathbb{Z}_p)$ s.t. $\Psi(h) = [a]$

$\Rightarrow \Psi$ is onto □

Rings

Definition A ring is an abelian group $(R, +, 0)$ together

a "multiplication" $\cdot$ so that

(1) $\cdot$ is associative: $\forall a,b,c \in R \quad (a\cdot b)\cdot c = a\cdot(b\cdot c)$

(2) $\cdot$ distributes over addition $+$: $\forall a,b,c \in R$

$$(a+b)\cdot c = (a\cdot c)+(b\cdot c), \qquad c\cdot(a+b) = (c\cdot a)+(c\cdot b)$$

Examples $(\mathbb{Z}, +, 0, \cdot)$, $(\mathbb{Z}_n, +, [0], \cdot)$, $\mathbb{Q}$, $\mathbb{R}$

Note • need not be commutative

$M_n(\mathbb{R})$ = $n\times n$ real matrices is a ring with the usual addition and multiplication of matrices.

Def A ring R is commutative if $a\cdot b = b\cdot a \quad \forall a,b \in R$.

Non-example $(\mathbb{R}^3, +, \vec{0}, \times)$ is not a ring: in general

$$\vec{v}\times(\vec{w}\times\vec{u}) \neq (\vec{v}\times\vec{w})\times\vec{u}$$

Def A ring R is a ring with unity if $\exists 1_R \in R$ s.t.

$$1_R \cdot a = a\cdot 1_R = a \quad \forall a \in R$$

Personal note I prefer my rings to have 1.

So for me $2\mathbb{Z}$ = even integers is not a ring.

For our textbook $2\mathbb{Z}$ is a ring.

Definition Let R be a ring (with 1). $u \in R$ is a unit if

$\exists v \in R$ s.t. $u\cdot v = 1$ and $v\cdot u = 1$

Notation $R^\times$ = the set of units of a ring R

Ex $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Z}_n^\times = \{[k] \in \mathbb{Z}_n \mid \gcd(k,n) = 1\}$

$\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$, $\mathbb{C}^\times = \{z \in \mathbb{C} \mid z \neq 0\}$

$(\mathbb{R}[x])^\times$ = constant nonzero polynomials

Remark In a ring R, $a \cdot 0 = 0 \quad \forall a \in R$

Proof $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$

Since $(R, +, 0)$ is an abelian group, $-(a \cdot 0)$ exists.

Add it to both sides. We get

$$-(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + (a \cdot 0) + (a \cdot 0)$$

$$\Rightarrow 0 = a \cdot 0.$$

Similarly $0 \cdot a = 0$.

If R is a ring with 1 and $0_R = 1_R$ then $\forall a \in R$

$$a = a \cdot 1_R = a \cdot 0_R = 0_R$$

$\Rightarrow R = \{0\}$.

From now on we assume: $\boxed{0_R \neq 1_R}$

Remark The set of units $R^\times$ is a group under multiplication (provided $1_R \in R$; which we'll assume from now on)

Definition A field is a commutative ring F (with 1) so that $\forall a \in F$, $a \neq 0$ is a unit.

Ex $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (p prime) are fields

$\mathbb{Z}_6$ is not a field: $[2]$ is not a unit.

$\mathbb{Z}$ is not a field

$\mathbb{R}[x]$ is not a field

Definition (6.1.7) Let R be a ring (with 1). A subset $S \subseteq R$ is a subring if 1) S is a subgroup of $(R, +, 0)$

(2) $1 \in S$ (3) $\forall a, b \in S$, $a \cdot b \in S$.

Note: If S is a subring of R then S is also a ring under the operations in R.

Ex $\mathbb{Z}$ is a subring of $\mathbb{Q}$

$\mathbb{R}$ is a subring of $\mathbb{R}[x]$ = ring of polynomials with real coefficients.

Def Let R, R' be two rings. A map $f: R \to R'$ is a **ring homomorphism** if f preserves $+$ and $\cdot$:

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)\,f(b)$$

$\forall\, a, b \in R$.

Ex $\pi: \mathbb{Z} \to \mathbb{Z}_n$, $\pi(k) = [k]$ is a ring homomorphism

Ex $f: \mathbb{R} \to M_2(\mathbb{R})$, $f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is a ring homomorphism.

$$f(a+b) = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

$$f(a \cdot b) = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

Note $f(1_{\mathbb{R}}) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{M_2(\mathbb{R})}$

Remark Any ring homomorphism $f: R \to R'$ is a homomorphism of groups: $(R, +, 0_R) \xrightarrow{f} (R', +, 0_{R'})$

So automatically $f(0_R) = 0_{R'}$.

But $f(1_R)$ need not equal $1_{R'}$ as we saw above.