3/11/16

<u>Λύση</u> (1ης Άσκησης)

$$H < \mathbb{Z}_p \times \mathbb{Z}_p \Rightarrow |H| = p$$

Έχω

$H_i = \langle (1,i) \rangle \quad i=1,\dots,p$

$H' = \langle (0,1) \rangle$

$\Big\}$ $p+1$ υποομάδες

Άρα

Θ.δ.ο. κάθε άλλη υποομάδα είναι μία από τις παραπάνω

Έστω $H'' = \langle (a,b) \rangle$, $(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_p$, $(a,b) \neq (0,0)$

Άρα $\exists h \in H''$ (Έστω $a \neq 0$)

$(a,b) \in H'' \Rightarrow \exists n \in \mathbb{N}$ ώστε

$(a,b)^n = (1, nb) \in H''$

$\exists i$ ώστε $H_i = H''$

<u>Λύση</u> (2ης Άσκησης)

Έστω O τ.ω. $|O| = 6$

- Έστω O κυκλική
  - $O \simeq \mathbb{Z}_6$
  - $\mathbb{Z}_3 \times \mathbb{Z}_2 \simeq \mathbb{Z}_6$, $(2,3)=1$

  $\Big\}$ $O \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$

- Έστω O όχι κυκλική

  $\exists a \in O \quad o(a) = 6 \quad |\langle a \rangle| = 6$

  $x, y \in O \quad o(x) = 2$

  $o(y) = 3$

Αν

$xy = yx : o(xy) = o(x)o(y) = 2 \cdot 3 = 6$

Αν $xy \neq yx$ έχουμε : e, x, y, y^2, xy, xy^2

- $x \neq y$, $x \cdot y \neq e$, $y \neq y^2$
- Αν $x = y^2$ $o(y) = o(y^2) = \frac{o(y)}{(o(y),2)} = \frac{3}{(3,2)} = 3$
- Αν $x = xy \Rightarrow y = e$
- Αν $x = xy \Rightarrow y^2 = e$
- Αν $y = xy \Rightarrow x = e$
- Αν $y^2 = xy^2 \Rightarrow x = e$
- Αν $y = xy^2 \Rightarrow xy = e \Rightarrow x^{-1} = y \Rightarrow o(x^{-1}) = o(x) = o(y)$
- Αν $y^2 = xy \Rightarrow x = y \rightarrow$ άτοπο.

Άρα $O = \{e, x, y, y^2, xy, xy^2\}$

$xy \neq e \Rightarrow x^{-1} = y$
$xy \neq x \Rightarrow x \neq e$
$yx \neq y \Rightarrow x \neq e$
$xy \neq yx$
$yx = y^2 \Rightarrow yx \in O \Rightarrow yx = xy^2$

Άρα

ισόμορφη με την Σ_3

Homework

Μετά από τις συμμετρικές 1, 2: $\forall m \geq n \ \exists Y \leq \Sigma_n$.
3, 4, 5, 6, 7.

Πρόταση

Αν σ και $\tau \in S_n$ κύκλοι ξένοι μεταξύ τους τότε $o(\sigma\tau) = [o(\sigma), o(\tau)] =$ Ε.Κ.Π.

Απόδειξη

$\sigma\tau = \tau\sigma \Rightarrow$

$a, b \in G$ με $ab = ba$ και

$(o(a), o(b)) = 1 \Rightarrow o(ab) = o(a)o(b)$

Από

την υπόθεση ισχύει το

$\sigma \cap \tau \neq \emptyset \Rightarrow \nexists\, k \in \mathbb{N}$ με $\sigma^k = \tau$

Έστω $o(\sigma\tau) = k \Rightarrow \sigma^k \tau^k = 1 \Rightarrow \sigma^k = (\tau^{-1})^k$

$$o(\sigma^k) = \frac{o(\sigma)}{(o(\sigma), k)} = \frac{o(\tau)}{(o(\tau), k)} \Rightarrow o(\sigma)(o(\tau), k) = o(\tau)(o(\sigma), k)$$

$$(\sigma\tau)^{o(\sigma)o(\tau)/(o(\sigma), o(\tau))} = \left(\sigma^{o(\sigma)}\right)^{\frac{o(\tau)}{(o(\sigma), o(\tau))}} \cdot \left(\tau^{o(\tau)}\right)^{\frac{o(\sigma)}{(o(\sigma), o(\tau))}} = 1$$

$\Rightarrow k \mid$ ΕΚΠ.

Θέλουμε

ΕΚΠ $\mid k \rightarrow$ Άσκηση για σ και τ όπως στην υπόθεση και a και b σε τυχαία ομάδα.

Πρόταση

Η S_n γεννάται από όλες τις αντιμεταθέσεις.

Η A_n —||— όλους τους κύκλους μήκους 3

Απόδειξη

$\sigma \in S_n \Rightarrow \sigma$ γινόμενο κύκλων ξένων

$\Rightarrow$ —||— αντιμεταθέσεων.

A_n = άρτιος

$\sigma \in A_n \Rightarrow \sigma$ γράφεται σαν άρτιο πλήθος αντιμεταθέσεων

Αρκεί

αυτά δύο να είναι γινόμενο κύκλων μήκους 3.

$$(i,j)(k,l) = \begin{cases} (i,j)(j,l) = (i,j,l) \\ \text{όλα διαφορετικά} \end{cases}$$

Άρα

$$(i,j)(k,l) = (i,j)(j,k)(j,k)(k,l) = (i,j,k)(j,k,l)$$

<u>Σώμα</u>

Έστω $\left\{ \mathbb{F} \text{ σώμα} \begin{array}{l} \nearrow (\mathbb{F},+) \\ \searrow (\mathbb{F},\cdot) \end{array} \right\} \subseteq \left\{ \begin{array}{l} \text{Διαιρετικοί δακτύλιοι} \\ \text{Όχι αντιμεταθετικοί} \end{array} \right\} \subseteq$

$\downarrow$

Ουσιαστικά χάνεται η αντιμεταθετ.

$\subseteq \left\{ \begin{array}{l} \text{χωρίς πρόσθεσ.} \\ \text{σαν πολλαπλασμός} \end{array} \right\}$

Γενικά ισχύει:

$$\mathbb{Q} < \underbrace{?\ ?}_{\text{υπάρχουν και άλλα σώματα}} < \mathbb{R} \leq \mathbb{C} \text{ δx}$$

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ ή $\mathbb{C}$ με πολλαπλασιασμό, όχι σώμα

$a+ib \leftrightarrow (a,b)$ $(a+ib)(a'+ib') = aa'-bb' + i(ab'+ba')$

πχ $x^2+1=0$

$$\mathbb{R}[x] \Big/ J = \langle (x^2+1) \rangle = \left\{ f(x)+J \,/\, f(x) \in \mathbb{R}[x] \right\} =$$

$$= \{a+bx(+J) \,/\, a,b \in \mathbb{R}\} = \{a+bi \,/\, a,b \in \mathbb{R}\} \Leftrightarrow \mathbb{C} \text{ δx διάστασης } 2$$

$$x+J = i \Rightarrow (x+J)^2 = x^2+J = -1+J \Leftrightarrow i^2 = -1$$

Με γινόμενο που έρχεται από τα σύμπλοκα

Ερώτημα

Ο $\mathbb{R}^3$ είναι σώμα?

Έχουμε $\mathbb{C} \equiv \mathbb{R}^2 \neq \mathbb{R}^3$

Αυτό σημαίνει πως ότι ιδιότητες είχε ο $\mathbb{R}^2$ θα τις κληρονομήσει και ο $\mathbb{R}^3$

Άρα $\mathbb{R}^3 = \langle 1, i, j \rangle = \{a+bi+cj \,/\, a, b, c \in \mathbb{R}\}$ $\quad i^2=-1$

$$i, j \in \mathbb{R}^3 \Rightarrow ij = a+bi+cj \Rightarrow$$

$$\Rightarrow iij = ai + bi^2 + cij$$

$$-j = ai - b + cij = ai - b + ca + cbi + c^2 j =$$

$$= -b + ca + (a+cb)i + c^2 j \Rightarrow c^2 = -1$$

Αδύνατο

άρα το $\mathbb{R}^3$ όχι σώμα

Ερώτημα

Είναι ο $\mathbb{R}^4$ σώμα?

$$\mathbb{R}^4 : \underbrace{\mathbb{R}}_{\text{ο χώρος αυτό τον αναφέρουμε για αυτό.}} / \langle 1, i, j, k \rangle_{\mathbb{R}}$$

Λύση

Εφοδιάζεται με γινόμενο?

Είναι το γινόμενο καλό? (Όχι μηδενοδιαιρέτες, αντιστροφές...)

$\mathbb{R} = \langle 1, i, j, k \rangle$

$\mathbb{R}^+$: στοιχεία ικανοπ. τάξης.

Στοιχεία πεπερ. τάξης :

Είναι στον $\mathbb{R}$ εδώ: $x^n=1 \Rightarrow |x|^n=1 \Rightarrow |x|=1 \Rightarrow x=\pm 1$

$\mathbb{C}^*$ στοιχεία πεπερ. τάξης

$x^n=1$: n-οστές ρίζες της μονάδας

άπειρα n μιας είναι στο μοναδιαίο κύκλο

$2 \to -1$

$4 \to i$

Αυτά τα στοιχεία μας δίνουν μια εικόνα για το τι μπορεί να έχει βάση

$Q_8 = \langle 1, i, j, k \rangle$

$o(i)=o(j)=o(k)=4$, $ij=k$

$ji=-k$

Άρα

$\mathbb{R}^4 \equiv \langle 1, i, j, k \rangle_{\mathbb{R}} = \mathbb{H}$ $\quad$ $\mathbb{H} \geq Q_8$ (Hamilton)

$\mathbb{C} \leq \mathbb{R}^4 \equiv \mathbb{H}$ $\quad$ γυρνάνε στα στοιχεία της βάσης.

$\boxed{a+bi+cj+k}$

Αν $a^2+b^2+c^2+d^2 \neq 0 \Rightarrow \exists$ αντίστροφος του $a+bi+cj+dk$

$$(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

Η διαφορά της ομάδας από το διανυσματικό χώρο είναι ότι στην ομάδα έχουμε μια πράξη, ενώ στο διανυσματικό χώρο δύο.

Πρόβλημα

Πόσοι πραγματικοί δακτύλιοι $(x \neq 0, \exists x^{-1})$ υπάρχουν πάνω από τους πραγματικούς
≡ Πόσες διαιρετικές άλγεβρες υπάρχουν?

1960 Adams:

Είναι n-διάστατος πραγματικός χώρος
δημιουργεί μια διαιρετική άλγεβρα
μόνο για $n=1,2,4,8$

$$\mathbb{R} \subsetneq \mathbb{C} \subsetneq \mathbb{H} \subsetneq \mathbb{K}\text{(aley)}$$

1962 Bott-Milnor

Ισχύει ότι είναι αυτές και μόνο αυτές.

Κάθε φορά που ανεβαίνω διάσταση, χάνεται και μια ιδιότητα.

Σύμπλοκα

$Y \leq O$ Δημιουργούμε τα σύμπλοκα

$$\left.\begin{array}{l} aY = \{ay \,/\, y \in Y\} \\ Ya = \{ya \,/\, y \in Y\} \end{array}\right\} \Rightarrow \text{όχι υποομάδες.}$$

Ορίζουμε σχέση ισοδυναμίας μεταξύ των στοιχείων μιας ομάδας O. $Y \leq O$

$$a \sim_Y b \Leftrightarrow ab^{-1} \in Y$$

Ομάδα ως προς κλάσεις ισοδυναμίας

1) $Ya = Yb \Leftrightarrow b \in Ya \Leftrightarrow ab^{-1} \in Y \Leftrightarrow ba^{-1} \in Y$
2) $Ya \cap Yb = \begin{cases} \emptyset \\ Ya = Yb \end{cases}$
3) $|Ya| = |Yb|$
4) Το πλήθος των αριστερών συμπλόκων ισούται με το πλήθος των δεξιών.

Απόδειξη

3) $|Ha| = |Hb| = |H|$

$\Phi : H \xrightarrow[\text{επί}]{1-1} Ha$ με $\Phi(g) = ga$

$ga = ga' \Longleftrightarrow a = a'$

$|H| = |Ha|$

$|Ha| = |aH| = |H|$

4) {δεξιά σύμπλοκα} $\xrightarrow{\Psi}$ {αριστερά σύμπλοκα}

$Ha \mapsto \Psi(H(a))^{-1} = a^{-1}H$

Η Ψ είναι 1-1 $a^{-1}H = b^{-1}H \Rightarrow Ha = Hb$, τα ίδια σύμπλοκα επί

$\forall\, aH \;\exists\, a'$ ώστε $\Psi(H(a^{-1})) = aH$

Τότε φαίνεται ο πληθικός αριθμός ανεξάρτητα από δεξιά ή αριστερά σύμπλοκα (γιατί είναι ο ίδιος και είναι ο δείκτης της ομάδας $[G:H]$ = πλήθος δεξιών ή αριστερών συμπλόκων)

$$G = \bigsqcup_{i \in I} a_i H = \bigsqcup_{i \in I} Ha_i \quad \text{με } |I| = [G:H]$$

Παράδειγμα

$S_3 \qquad H = \langle g \rangle \qquad o(g) = 2$

$$[S_3 : H] = \frac{\text{πλήθος της } S_3}{\text{πλήθος της } H} = \frac{6}{2} = 3$$

$$\left.\begin{array}{l} H = \{1, g\} \\ Hf = \{f, gf\} \\ Hf^2 = \{f^2, f^2 g\} \end{array}\right\} S_3 = H \sqcup Hf \sqcup Hf^2$$

Παράδειγμα

$$n\mathbb{Z} \le \mathbb{Z} = n\mathbb{Z} \sqcup (1+n\mathbb{Z}) \sqcup \dots \sqcup (n-1+n\mathbb{Z})$$

$$a\in\mathbb{Z} \Rightarrow a = n\cdot\pi + u \qquad 0 \le u \le n-1$$

$$a+n\mathbb{Z} = (n\pi+u)+n\mathbb{Z} = u+n\mathbb{Z}$$

↳ από εδώ βγαίνει το mod

$\mathbb{Z}/n\mathbb{Z}$ ή $\mathbb{Z}_n = \{a+n\mathbb{Z} / a\in\mathbb{Z}\}$

$$[\mathbb{Z} : n\mathbb{Z}] = n$$

Παράδειγμα

$$\mathbb{Z} \le \mathbb{Q} \qquad [\mathbb{Q}:\mathbb{Z}] = +\infty$$

Έστω

$$r\in\mathbb{Q} \Rightarrow r = [r]+r' \qquad 0 \le r' < 1$$

$$r+\mathbb{Z} = [r]+r'+\mathbb{Z} = r'+\mathbb{Z} \qquad 0 < r+r' < 1$$

$\Rightarrow r'+\mathbb{Z} = r''+\mathbb{Z} \ \forall r'$ με $0 \le r' < 1$

Έχεις διαφορετικά σύμπλοκα $\Rightarrow [\mathbb{Q}:\mathbb{Z}] = +\infty$

Θεώρημα (Lagrange)

Αν G: ομάδα με $|G| < +\infty$ τότε κάθε υποομάδα της έχει τάξη διαιρέτη της $|G|$

Πόρισμα

Αν G ομάδα με $|G| = p$ πρώτος και κάθε στοιχείο της διαφορετικό από το μοναδιαίο, είναι γεννήτορες.

Απόδειξη

Αν G όχι κυκλική $\Rightarrow \exists\ a,b\in G$ με $b \neq a^k$

$\forall k\in\mathbb{Z} \Rightarrow \left.\begin{array}{l} |\langle b\rangle| / |G| \\ |\langle a\rangle| / |G| \end{array}\right\}$ δύο διαφορετικούς διαιρέτες του p αδύνατον

Άρα $G = \langle a\rangle$

Θεώρημα (Fermat)

Αν p: πρώτος και $\alpha \in \mathbb{Z}$ με $(\alpha, p) = 1$, τότε $\alpha^{p-1} \equiv 1 \bmod p$.

Σχόλιο:

$\mathbb{Z}_n$: κυκλική

$\mathbb{Z}_n^*$: δεν ορίζεται

$\mathbb{Z}_p^*$: κυκλική (πρωταρχικά στοιχεία από θεωρία αριθμών)