Homework 21.

#1

a) $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$

$f: \mathbb{C} \to \mathbb{R}$

$z \mapsto Im(z)$

$Im(z_1 z_2) = Im(z_1) \cdot Im(z_2)$ - гомоморфизм.

$\mathbb{C}/\mathbb{R} \cong \mathbb{R}$

$\uparrow\!\!\uparrow$

$Im\, f = \mathbb{R}$, т.к. $Im(z) = b \in \mathbb{R}$

$Ker\, f = \{ z \in \mathbb{C} \mid Im(z) = 0 \} \in \mathbb{R}$, т.к. тогда $z = a + bi$, где $a, b \in \mathbb{R}$

c) $\mathbb{C}^\times/U \cong \mathbb{R}^\times_{>0}$ $\quad |z_1 z_2| = |z_1|\cdot|z_2|$ – гомоморфизм

$f: \mathbb{C}^\times \to \mathbb{R}^\times_{>0}$

$z \mapsto |z|$

такие $z \in \mathbb{C}^\times$, что $\sqrt{a^2+b^2} = 1$, где $z = a+bi$, $a, b \in \mathbb{R}$

$\operatorname{Ker} f = U$

$\operatorname{Im} f = \mathbb{R}^\times_{>0}$ $\Rightarrow \mathbb{C}^\times/U \cong \mathbb{R}^\times_{>0}$

$|z| = \sqrt{a^2+b^2} \in \mathbb{R}$

b) $\mathbb{C}^\times/U_n \cong \mathbb{C}^\times$

$f: \mathbb{C}^\times \to \mathbb{C}^\times$ $\quad (z_1 z_2)^n = z_1^n \cdot z_2^n$ – гомоморфизм

$z \mapsto z^n$

$\operatorname{Ker} f = \{ z \in \mathbb{C}^\times \mid z^n = 1 \}$

$\operatorname{Im} f = \mathbb{C}^\times$, т.к. $z^n = r^n \cdot e^{i2\pi n} \in \mathbb{C}^\times$ $\Rightarrow \mathbb{C}^\times/U_n \cong \mathbb{C}^\times$

#2.

$G = GL_n(\mathbb{R})$ $\quad A = \{ X \in G \mid |\det X| = 1 \}$

$H = GL_n(\mathbb{C})$ $\quad C = \{ X \in H \mid |\det X| = 1 \}$

a) $G/A \cong \mathbb{R}^\times_{>0}$

$f: G \to \mathbb{R}^\times_{>0}$ $\quad |\det L_{n_1} \cdot \det L_{n_2}| = |\det L_{n_1}| \cdot |\det L_{n_2}|$

$L_n \mapsto |\det L_n|$

$\operatorname{Ker} f = \{ L_n \mid |\det L_n| = 1 \}$

$\operatorname{Im} f = \{ |\det L_n| > 0 \}$ $\Rightarrow G/A \cong \mathbb{R}^\times_{>0}$

(при $\det L_n = 0$ матрица тривиальна

b) $H/C \cong \mathbb{R}^*_{>0}$

$f: H \to \mathbb{R}^*_{>0}$ $\qquad |\det L_{n_1} \cdot \det L_{n_2}| = |\det L_{n_1}| \cdot |\det L_{n_2}|$

$L_n \mapsto |\det L_n|$

$\operatorname{Ker} f = \{ L_n \in GL_n(\mathbb{C}) \mid |\det L_n| = 1 \}$

$\operatorname{Im} f = \{ |\det L_n| > 0 \}$

$\Rightarrow H/C \cong \mathbb{R}^*_{>0}$

#7.

$G = \mathbb{Z}_{13}^*$ $\qquad g = \bar{2}$ $\qquad a = 5$

a) $2^1 \equiv 2$ $\qquad 2^5 \equiv 6$ $\qquad 2^9 \equiv 5$

$2^2 \equiv 4$ $\qquad 2^6 \equiv 12$ $\qquad 2^{10} \equiv 10$

$2^3 \equiv 8$ $\qquad 2^7 \equiv 11$ $\qquad 2^{11} \equiv 7$ $\qquad \pmod{13}$

$2^4 \equiv 3$ $\qquad 2^8 \equiv 9$ $\qquad 2^{12} \equiv 1$

$\Rightarrow \operatorname{ord}(g) = 12$

b) Сообщили мне $\bar{9} \Rightarrow 9 = 2^8 \pmod{13} \Rightarrow g^b = 9;\ b = 8$

~~Общий ключ: $g^{ab} = 2^{5 \cdot 8} \equiv (2^5)^8 \equiv 6^8 \equiv 2^8 \cdot 3^8 \equiv 2^8 \cdot (3^2)^4 \equiv$~~

~~$\equiv g \cdot (g)^4 \equiv g \cdot (-4)^4 \equiv g \cdot 2^8 \equiv g \cdot g \equiv 81 \equiv$~~

Общий ключ: $g^a \cdot g^b = \bar{2}^5 \cdot \bar{2}^8 = \bar{6} \cdot \bar{9} = \overline{54} = \bar{2}$

Ответ: $\operatorname{ord}(g) = 12$; $g^{ab} = \bar{2}$; $b = 8$

#8.

$G = \mathbb{Z}_{17}^{\times}$ $\quad g = \bar{3}$ $\quad a = 8$

a) $3^1 \equiv 3$ $\quad 3^5 \equiv 5$ $\quad 3^9 \equiv 14$ $\quad 3^{13} \equiv 12$

$3^2 \equiv 9$ $\quad 3^6 \equiv 15$ $\quad 3^{10} \equiv 8$ $\quad 3^{14} \equiv 2$ $\pmod{17}$

$3^3 \equiv 10$ $\quad 3^7 \equiv 11$ $\quad 3^{11} \equiv 7$ $\quad 3^{15} \equiv 6$

$3^4 \equiv 13$ $\quad 3^8 \equiv 16$ $\quad 3^{12} \equiv 4$ $\quad 3^{16} \equiv 1$

$\Rightarrow ord(g) = 16.$

b) B сообщил $\bar{4}$

Закодировал h парой $(\bar{8}, \bar{11})$

A сообщил $g^a = \bar{3}^8 = \bar{16}$

$(\bar{8}, \bar{11}) = (g^k, h \cdot (g^a)^k) \Rightarrow \bar{3}^k = \bar{8} \Rightarrow k = 10$

~~$h \cdot g^{ab} = \bar{11} \quad g^{ab} \equiv \bar{3}^{a \cdot b} = \bar{16} \cdot \bar{3}^{10} \equiv \bar{16} \cdot \bar{8} = \bar{128} = \bar{9}$~~

$h \cdot g^{ak} \cdot (g^k)^{|G|-a} = \bar{11} \cdot g^{8 \cdot 10} \cdot (g^{10})^{16-8} = \bar{11} \cdot g^{16 \cdot 5} \cdot g^{16 \cdot 5} \equiv \bar{11} \cdot \bar{1} \cdot \bar{1} = \bar{11}$

$h \cdot g^b = k$

$\bar{11} \cdot g^b = \bar{10}$

$\bar{3}^7 \cdot \bar{3}^b = \bar{3}^3$

$7 + b = 3 \Rightarrow b = -4 \equiv 12 \mod 16$, т.к. $ord(g) = 16$

Ответ: $ord(g) = 16$, $h = \bar{11}$, $k = 10$, $b = 12$.

#3.

a) $G = GL_n(\mathbb{R})$ $\quad H = SL_n(\mathbb{R})$

$gH = Hg \quad \forall g \in G \Rightarrow H \triangleleft G$

$\Updownarrow$

$gHg^{-1} \in H$ – докажем это

$\det(gHg^{-1}) = \det g \cdot \underbrace{\det H}_{=1} \cdot \det g^{-1} = \det g \cdot \det g^{-1} = 1 \Rightarrow$

$\Rightarrow gHg^{-1} \in H \Rightarrow H \triangleleft G$

b) $G = S_n$ $\quad H = A_n$

$|S_n| = n!$ $\quad |A_n| = \frac{n!}{2}$

Рассмотрим $gHg^{-1} \quad \forall g \in G$

$|gHg^{-1}| = |g| \cdot |H| \cdot |g^{-1}| = n! \cdot \frac{n!}{2} \cdot \frac{1}{n!} = \frac{n!}{2} \Rightarrow gHg^{-1} \in H$

$\Rightarrow H \triangleleft G$

#4.

$a \in G$ $\quad$ Док-ть: $Z_G(a) \leq G$

1) $\forall a \in G : a \cdot e = e \cdot a = a \in G \Rightarrow e$ коммутирует с $a \Rightarrow e \in Z_G(a)$

2) $\forall g \in Z_G(a) : g^{-1} \in Z_G(a)$

Возьмём $g \in Z_G(a)$: $ag = ga \Rightarrow$ $g^{-1}ag = a \Rightarrow g^{-1}a = ag^{-1}$

($\cdot g^{-1}$ слева) ($\cdot g^{-1}$ справа)

$\Rightarrow g^{-1}$ коммутирует с $a \Rightarrow g^{-1} \in Z_G(a)$

3) Хотим $g, h \in Z_G(a) : gh \in Z_G(a)$

Пп: $gh \notin Z_G(a)$, но $\left.\begin{matrix} ag = ga \\ ah = ha \end{matrix}\right\} \Rightarrow \left.\begin{matrix} gag^{-1} = a \\ hah^{-1} = a \end{matrix}\right\} \Rightarrow$

$\Rightarrow (gh)\,a\,(gh)^{-1} = g\underbrace{hah^{-1}}_{=a}g^{-1} = gag^{-1} = a \in Z_G(a)$

$\Rightarrow (gh)a = a(gh) \Rightarrow gh$ комм. с $a \Rightarrow gh \in Z_G(a)$

3 условия выполнены $\Rightarrow Z_G(a) \leq G$

#5.

G – невырожд. верхнетреуг. матрицы

$$H = E + \sum_{\substack{1 \le i < j \le n \\ j - i \ge k}} a_{ij} E_{ij}, \quad a_{ij} \in \mathbb{R}$$

$H \subseteq G$

Должно выполняться: $gHg^{-1} \in H$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & & \vdots \\ & & \ddots & \\ & 0 & & a_{n-k,n} \\ 0 & & & a_{nn} \end{pmatrix} \begin{pmatrix} 0 & \cdots & b_{1,1+k} & \cdots \\ & 0 & \ddots & \vdots \\ & & \ddots & b_{n-k,n} \\ & 0 & & 0 \end{pmatrix} \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ 0 & c_{22} & & \\ \vdots & & \ddots & \\ 0 & & & c_{nn} \end{pmatrix} =$$

какие-то числа после умножения gH

$$= \begin{pmatrix} 0 & 0 & * & * & * \\ 0 & 0 & 0 & \ddots & * \\ \vdots & \vdots & \vdots & 0 & * \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}^{k+1} \begin{matrix} \\ \\ \\ \\ n-k \end{matrix} \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ & c_{22} & \vdots \\ 0 & & c_{nn} \end{pmatrix} = \begin{pmatrix} 0 & 0 & * & * & * \\ 0 & 0 & \ddots & * & * \\ \vdots & \vdots & & \ddots & * \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}^{k+1} \begin{matrix} \\ \\ \\ \\ n-k \end{matrix} \in H$$

$\Rightarrow gHg^{-1} \in H \Rightarrow H \lhd G$

#6.

G – невырожденные верхнетреугольные матрицы

$$Z(G) = \{a \in G \mid ga = ag \quad \forall g \in G\}$$

Для $\forall g$ будет выполнено $ga = ag$, если $a \in \{\lambda \cdot E \mid \lambda \in \mathbb{R}\}$,

т.к. единичная матрица коммутирует с любой матрицей.

Также её можно домножить на коэффициент $\lambda \in \mathbb{R}$.

(который можно вынести за матрицу и перемножить; получится: $a \cdot (\lambda E) = \lambda \cdot (aE) = (a \cdot E) \cdot \lambda = (Ea) \cdot \lambda = \lambda (Ea) = (\lambda E) a$)

Ответ: $\{\lambda \cdot E \mid \lambda \in \mathbb{R}\}$.