Answer sheet 5 - Yiwei Yang 2018533218

1.

a.

I'll show that $[SL_n(\mathbb{R}), SL_n(\mathbb{R})] = SL_n(\mathbb{R})$. that is to say $SL_n(\mathbb{R})$ is perfect. Let k be a field. $SL(n,k)$ is the special linear group over k.

First, elementary matrices of the first kind generate the special lineasr group over a field. The group of invertible $n*n$ matrices over k with determinant equal to 1. Then $SL(n,k)$ is generated by elementary matrices of form $E_{i,j}$, where $\lambda \in K, 1 \leq i,j \leq n, i \neq j$. By useal Gauss-Jordan ellimination, the matrix $E_{i,j}(\lambda)$ has 1s on the diagonal, λ in the $(ij)^{th}$ position and 0 elsewhere.

Then for $n \geq 2$ number, for $i \neq j$ in the set $\{1,2,\ldots n\}$ and $\lambda \in k$, let $e_{ij}(\lambda)$ be the matrix with λ in the $(ij)^{th}$ position and 0 elsewhere, $E_{ij}(\lambda)$ be termed elementary matrices and $\in SL_n k \forall i \neq j, \lambda \in k$

1. If $n \geq 3$, every elementary matrix can be expressed as a commutator of two elementary matrices. In particular, it is the commutator of two elements of $SL_n(k)$.
   Pick $l \in \{1,2,3,\ldots,n\}$ different from i, j. Consider elements:
   $g = E_{il}(\lambda), \quad h = E_{lj}(1)$
   Then, the commutator is given by:
   $ghg^{-1}h^{-1} = E_{il}(\lambda)E_{lj}(1)E_{il}(-\lambda)E_{lj}(-1)$
   Rewriting in terms of the e_{ij} s:
   $ghg^{-1}h^{-1} = (I + e_{il}(\lambda))\,(I + e_{lj}(1))\,(I - e_{il}(\lambda)))\,I - e_{lj}(1))$
   Simplifying this yields:
   $ghg^{-1}h^{-1} = (I + e_{il}(\lambda) + e_{lj}(1) + e_{ij}(\lambda))\,(I - e_{il}(\lambda) - e_{lj}(1) + e_{ij}(\lambda))$
   Further simplification yields:
   $ghg^{-1}h^{-1} = I + e_{ij}(\lambda) = E_{ij}(\lambda)$
2. If $n = 2$, and k has more than three elements, every elementary matrix can be expressed as a commutator of two elements of $SL_n(k)$.
   If k has more than three elements, there exists $\mu \in k$ such that μ is invertible and $\mu^2 \neq 1$.
   We need to prove that for any λ, the element $E_{12}(\lambda)$ (and analogously, the element $E_{21}(\lambda)$) is expressible as a commutator. Indeed, set:
   $$g = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}, \quad h = \begin{pmatrix} 1 & \frac{\lambda}{\mu^2-1} \\ 0 & 1 \end{pmatrix}.$$
   A computation shows that the commutator of g and h is $E_{12}(\lambda)$. A similar construction gives $E_{21}(\lambda)$ as a commutator.$\square$

b.

If $n = 2$, we apply the commutator relation, $[\begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}] = \begin{pmatrix} 1 & (\mu^2-1)\tau \\ 0 & 1 \end{pmatrix}$ but for any $\lambda \in k$, we have $\lambda = (\mu^2 - 1)\tau$. This can be solved for τ as long as there exists a unit $\mu \in k^{x}$ so that $\mu \neq \pm 1$. this only works with at least 3 elements in k^{x}. $\square$

2.

a.

For $(\mathbb{Z}/n\mathbb{Z}, \mathrm{x}, \cdot)$, if n is a composite number, then there are $1 < a, b < n$ such that $ab = n$. Hence $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$
are non-zero and their product is zero. So $\mathbb{Z}/n\mathbb{Z}$ has zero-divisors.

If p is prime, then $p \mid ab$ if and only if either $p \mid a$ or $p \mid b$. Hence $\mathbb{Z}/p\mathbb{Z}$ is a unital (non-trivial) commutative ring without zero-divisors.

If $n = 1$, then $\mathbb{Z}/n\mathbb{Z}$ is the trivial ring which is not an integral domain (by the definition).

b.

First, 1 plays the same role in multiplication as o does in addition: $1 \times a = a, 0 + a = a$. They are called
the identity. (o is the additive identity in $\mathbb{Z}_{30}$, 1 is the multiplicative identity in $\mathbb{Z}_{31}^{\times}$).

Then look into $(\mathbb{Z}_{31})^*$ in detail. For $[1]$, it's clearly the multiplicative idnetity. For $[2]$, $[2]^5 \equiv 1(mod\ 31)$, so order is 5. For $[3]$, $[3]^30 = [1]$

So 3 generates the whole group $\mathbb{Z}_{31}^{\times}$.$\square$

c.

No integer solution.

It's a well known and pretty useful fact that the only possible remainders when a perfect cube is divided by 9 are -1,0 and 1 (we can easily prove it using Euclid's division lemma and then checking remainders of the first nine cubes).
That is, for an integer n we have,
$n^3 \equiv \pm 1(mod\ 9)$ when n is not divisible by 3
and, $n^3 \equiv 0(mod\ 9)$ when n is divisible by 3.

Since, each of the cubes can only take any one of the values of -1,0 and 1, so the all possible values of $x^3 + y^3 - z^3(mod\ 9)$ are -3,-2,-1,0,1,2 and 3, but $x^3 + y^3 - z^3 \equiv 4$, which is contradiction.$\square$

3.

a.

Denote $N = \bigcap_{g \in G} gHg^{-1}$ be the family of all normal subgroups of G contained in H. The family is non-empty, since $1 \subseteq H$ is a normal subgroup of G. We claim $N \ = \Sigma_{\lambda \in \Lambda} N_\lambda$, the group generated by all the N_λ's, satisfied the conditions given. First, since $N_\lambda \subseteq H$ for each $\lambda \in \Lambda$, clearly we also have $N \subseteq H$. Every normal subgroup of G contained in H is one of the N_λ, which is by definition contained in N. Thus, since an element of N is of the form $h_1, h_2 \ldots h_m$, where $h_n \in N_{\lambda_n}$, for each $g \in G$, we have $g(h_1 h_2 \ldots h_n)g^{-1} = (gh_1 g^{-1})(gh_2 g^{-1}) \ldots (gh_n g^{-1}) \subseteq N$, N is a normal subgroup of G.

b.

If N is a normal subgroup of group G and $n \in N$ then $gng^{-1} \in N$ for every $g \in G$ or equivalently $[n] \subseteq N$ where $[n] := \left\{gng^{-1} \mid g \in G\right\}$ is the conjugacy class of n.
This tells us that:

N is normal $\Leftrightarrow \forall g \in G, N = gNg^{-1}$

$\Leftrightarrow \forall n \in N \forall g \in G \exists m_{n,g} \in N, n = g m_{n,g} g^{-1}$
$\Leftrightarrow N = \bigcup_{n \in N} \underbrace{\bigcup_{g \in G} \{g m_{n,g} g^{-1}\}}_{\text{conjugacy class of } n}$
$\Leftrightarrow N = \bigcup_{n \in N} [n],$

If conversely N is a subgroup of group G that satisfies $N = \bigcup_{n \in N} [n]$ then it is immediate that $gng^{-1} \in N$ for every $n \in N$ and $g \in G$.$\square$

4.

$\rightarrow$: For G, we have $\forall w \in G, w^3 = 1$, thus $aca^{-1}c^{-1} = a^2ba^2b^2a^2bab^2a^2 = (a^2b)^2 ba(ab)^2ba^2 = b(ba)^2b(ba^2)^2 = ba^2b^2bab^2 = 1$ so $ac = ca$, and similarly $bc = cb$. Also, we have $cba = ab$, so $ba = c^{-1}ab = abc^2$.

By the way, any word in G can be written in the form $a^ib^jc^k$ with $i, j, k \in \{0, 1, 2\}$, which means that G is finite with $|G| \leq 27$. To get equality, note that the Heisenberg group H on $\mathbb{F}_3$ is generated by two elements and every non-identity element has order 3 . This means that H is some quotient of G, hence $|G| \geq |H| = 27$.

$\leftarrow$: Write $(z_1, z_3; z_2) = \begin{pmatrix} 1 & z_1 & z_2 \\ & 1 & z_3 \\ & & 1 \end{pmatrix}$

it suffices to check that $(z_1, z_3; z_2)(x, z; y)^{-1} \in G$. But $(x, z; y)^{-1} = (-x, -z; xz - y)$ and $(z_1, z_3; z_2)(-x, -z; xz - y) = (z_1 - x, z_3 - z; z_2 - cz + xz - y) \in G$.$\square$