S.-T. Yau College Student Mathematics Contests 2023

Algebra and Number Theory

Solve every problem.

1. Let F be a field. Let $n \geq 2$ be an integer. For $1 \leq i \neq j \leq n$ and for $\lambda \in F$, set $E_{ij}(\lambda) = (e_{kl})$ the following $n \times n$-matrix such that

$$e_{kl} = \begin{cases} 1, & \text{if } k = l; \\ \lambda, & \text{if } (k,l) = (i,j); \\ 0, & \text{otherwise.} \end{cases}$$

   (1) Show that the special linear group $\mathbf{SL}_n(F)$ can be generated by the matrices $E_{ij}(\lambda)$ ($1 \leq i \neq j \leq n$ and $\lambda \in F$).

   (2) Assume $n \geq 3$. Show that the general linear group $\mathbf{GL}_n(F)$ is not solvable. **Hint**: one can start by computing the commutators of the matrices $E_{ij}(\lambda)$.

   (3) Assume $n = 2$ and F is a field containing at least 4 elements. Show that $\mathbf{GL}_n(F)$ is not solvable either. **Hint**: one can start by computing the commutator of the matrix $E_{12}(\lambda)$ with a diagonal matrix.

   (4) Let $\mathbb{F}_q$ denote the finite field with q elements. Are $\mathbf{GL}_2(\mathbb{F}_2)$ and $\mathbf{GL}_2(\mathbb{F}_3)$ solvable? Justifiy your assertion.

2. Let R be a ring with identity $1 \neq 0$.

   (1) Assume that R is commutative. Show that, if we have an isomorphism $R^n \simeq R^m$ of R-modules for some positive integers n and m, then $m = n$.

   (2) The analogous assertion of (1) for a non-commutative ring is not true in general as shown by the following example (in particular, the notion of "rank" of a finite free module over such rings is not well-defined). Let K be a non-trivial (not necessarily commutative) ring with identity, and F be a free K-module with a countable basis indexed by $\mathbb{Z}_{\geq 1}$:

$$e_1, \ldots, e_2, \ldots, e_n \ldots.$$

   Write $R = \mathrm{End}_K(F)$, which is a ring with the usual addition and composition of two K-linear endomorphisms of F.

   (a) Show that R is not commutative.

   (b) Let $f_0 \in R$ (resp. $f_1 \in R$) such that $f_0(e_{2i}) = e_i$ and $f_0(e_{2i-1}) = 0$ (resp. $f_1(e_{2i}) = 0$ and $f_1(e_{2i-1}) = e_i$) for every $i \in \mathbb{Z}_{\geq 1}$. Show that $\{f_0, f_1\}$ is a basis of R as a left R-module (given by left-multiplication).

   (c) For any integers $n, m \geq 1$, show that there exists an isomorphism $R^n \xrightarrow{\sim} R^m$ of R-modules.

3. Let G be a profinite gorup. We say that it is *topologically finitely generated* if there exist finitely many elements $g_1, \ldots, g_n$ such that the closed subgroup generated by $g_1, \ldots, g_n$ is equal to G.

   (1) Assume that G is topologically finitely generated. Show that, for a fixed positive integer n, G has only finitely many open subgroups of index n.

   (2) Show that, for K a number field (i.e., a finite field extension of $\mathbb{Q}$), its absolute Galois group G_K is not topologically finitely generated.

4. Let R be a commutative ring with identity. An R-module M is said to be of *finite presentation* if there exists an exact sequence of R-modules

$$R^n \longrightarrow R^m \longrightarrow M \longrightarrow 0$$

   for some positive integers $m, n \geq 0$.

   (1) Let $f : N \to M$ be a surjective morphism of R-modules with N of finite type and M of finite presentation. Show that the R-module $\ker(f)$ is of finite type.

   (2) Let M be an R-module of finite type. Show that the following statements are equivalent.

      (a) M is flat and of finite presentation.

      (b) M is locally free, i.e., there exist $f_1, \ldots, f_s \in R$ generating the unit ideal of R such that M_{f_i} is free over R_{f_i}.

      (c) M is projective as an R-module.

   (3) Let $S = \prod_{\mathbb{N}} R$ the product of countably many copies of R, and $I = \oplus_{\mathbb{N}} R \subset S$. Show that S/I is a flat S-module which is not projective.

5. Let p be a prime number. Let $\mathbb{Z}_p$ be the ring of p-adic integers.

   (1) Let $a \in \mathbb{C}$ such that $\lim_{r \to \infty} a^{p^r} = 1$. Show that a is a p^m-th root of unity for some m.

   (2) Let $A \in \mathbf{M}_{n \times n}(\mathbb{C})$ be an $n \times n$ complex matrix such that $\lim_{r \to \infty} A^{p^r} = I_n$, with I_n the identity matrix. Show that $A^{p^m} = I_n$ for some integer m.

   (3) Determine, up to isomorphisms, all the finite-dimensional continuous complex representations of $\mathbb{Z}_p$.

6. Let p be a prime number. Let K be a p-adic local field, i.e., a finite field extension of $\mathbb{Q}_p$. Denote by $\mathcal{O}_K$ its ring of integers, with $\pi \in \mathcal{O}_K$ a uniformizer.

   (1) Show that, the following logarithm map

$$\log : 1 + p\mathcal{O}_K \longrightarrow p\mathcal{O}_K, \quad 1 + x \mapsto x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots$$

   is a well-defined isomorphism of groups, which can be extended in a unique way to a group homomorphism

$$\log_\pi : K^\times \longrightarrow K,$$

   such that $\log_\pi(\pi) = 0$. Determine the kernel of $\log_\pi$.

   (2) With the help of the logarithm above, show that for any integer $n \geq 1$, the group quotient $K^\times / K^{\times, n}$ is a finite group.