# Algebra, Number Theory and Combinatorics (2021)

**Problem 1.** (Individual round.) Let $p$ be a prime number and $\mathbb{Q}_p$ the field of $p$-adic numbers. Let $n \geq 1$ be an integer and $L = \mathbb{Q}_p(\zeta_{p^n})$, where $\zeta_{p^n}$ denotes a primitive $p^n$-th roots of unity. Determine the image of the norm map $N_{L/\mathbb{Q}_p} : L^\times \to \mathbb{Q}_p^\times$. You may use the inequality $[L : \mathbb{Q}_p] \leq (\mathbb{Q}_p^\times : N_{L/\mathbb{Q}_p}(L^\times))$ without proof in the case $n \geq 2$.

**Problem 2.** (Individual round.) Let $k$ be a field and $V$ a $k$-vector space of dimension $n$. Consider the group homomorphism:

$$\phi : \mathrm{GL}(V) \to \mathrm{GL}(\wedge^2 V), f \mapsto \wedge^2 f.$$

(1) Determine the kernel of $\phi$.

(2) Show that $\phi$ induces a group homomorphism $\psi : \mathrm{SL}(V) \to \mathrm{SL}(\wedge^2 V)$. Express $det(\wedge^2 f)$ in terms of $det(f)$.

**Problem 3.** (Individual round.) Let $A$ be a rank 2 integer matrix of size $5 \times 3$. Classify all possible groups of the form $\mathbb{Z}^5 / A\mathbb{Z}^3$.

**Solution to Problem 1.** We will show that $N_{L/\mathbb{Q}_p}(L^\times) = p^{\mathbb{Z}}(1+p^n\mathbb{Z}_p)$, where $\mathbb{Z}_p$ denotes the ring of $p$-adic integers.

Let $\Phi(X) = (X^{p^n}-1)/(X^{p^{n-1}}-1)$ be the $p^n$-th cyclotomic polynomial. Then $\Phi(X+1)$ is an Eisenstein polynomial. Thus $\Phi(X)$ is the minimal polynomial of $\zeta_{p^n}$, so that

$$N_{L/\mathbb{Q}_p}(1-\zeta_{p^n}) = \Phi(1) = p.$$

We have $[L:\mathbb{Q}_p] = \phi(p^n) = p^n - p^{n-1}$. For $p$ odd, the $\phi(p^n)$-th power map on $1+p\mathbb{Z}_p$ is the composition

$$1+p\mathbb{Z}_p \xrightarrow[\sim]{\log} p\mathbb{Z}_p \xrightarrow[\sim]{\phi(p^n)} p^n\mathbb{Z}_p \xrightarrow[\sim]{\exp} 1+p^n\mathbb{Z}_p.$$

Thus

$$N_{L/\mathbb{Q}_p}(L^\times) \supseteq N_{L/\mathbb{Q}_p}(1+p\mathbb{Z}_p) = 1+p^n\mathbb{Z}_p.$$

For $p=2$, we may assume $n \geq 2$. The $\phi(2^n)$-th power map on $1+4\mathbb{Z}_2$ is the composition

$$1+4\mathbb{Z}_2 \xrightarrow[\sim]{\log} 4\mathbb{Z}_2 \xrightarrow[\sim]{\phi(2^n)} 2^{n+1}\mathbb{Z}_2 \xrightarrow[\sim]{\exp} 1+2^{n+1}\mathbb{Z}_2.$$

Thus

$$N_{L/\mathbb{Q}_2}(L^\times) \supseteq N_{L/\mathbb{Q}_2}(1+4\mathbb{Z}_2) = 1+2^{n+1}\mathbb{Z}_2.$$

It is easy to see that

$$1+2^n\mathbb{Z}_2 = (1+2^{n+1}\mathbb{Z}_2)\coprod 5^{2^{n-2}}(1+2^{n+1}\mathbb{Z}_2)$$

and

$$5^{2^{n-2}} = N_{L/\mathbb{Q}_2}(2+\zeta_4).$$

This finishes the proof of $N_{L/\mathbb{Q}_p}(L^\times) \supseteq p^{\mathbb{Z}}(1+p^n\mathbb{Z}_p)$ in all cases.

Let $\mathcal{O}_L$ denote the integral closure of $\mathbb{Z}_p$ in $L$. The residue field of $L$ is $\mathbb{F}_p$, so that $N_{L/\mathbb{Q}_p}|_{\mathcal{O}_L^\times}$ is compatible with the $\phi(p^n)$-th power map on $\mathbb{F}_p^\times$, which carries every element to 1. In other words, $N_{L/\mathbb{Q}_p}(L^\times)\cap\mathbb{Z}_p^\times = N_{L/\mathbb{Q}_p}(\mathcal{O}_L^\times) \subseteq 1+p\mathbb{Z}_p$. This finishes the proof in the case $n=1$. For $n\geq 2$, it suffices to apply the given inequality $(\mathbb{Q}_p^\times : N_{L/\mathbb{Q}_p}(L^\times)) \geq \phi(p^n) = (\mathbb{Q}_p^\times : p^{\mathbb{Z}}(1+p^n\mathbb{Z}_p))$. □

**Solution to Problem 2.** (1) If $n=2$, then $\wedge^2 V \simeq k$ and $\phi(f)\in \mathrm{GL}(k)$ is just the multiplication by $det(f)$, hence the kernel is just $\mathrm{SL}(V) = \mathrm{SL}_2$. Now assume $n\geq 3$. By definition, $f\in \mathrm{Ker}(\phi)$ if and only if $f(x)\wedge f(y) = x\wedge y$ for all $x,y\in V$. We claim $x$ and $f(x)$ are proportional: otherwise expand to a basis $e_1 = x, e_2 = f(x), e_3, ..., e_n$, then we have $e_2\wedge f(e_3) = e_1\wedge e_3$ which is not possible as $e_i\wedge e_j$ is a basis of $\wedge^2 V$. Hence $x$ and $f(x)$ are proportional for all $x\in V$. This implies that $f(x) = ax$ for some $a\in k$. Then $f(x)\wedge f(y) = a^2 x\wedge y = x\wedge y$, thus $a = \pm 1$. So the kernel is just $\pm Id$.

(2) First we show the case for elementary matrices: Take a basis $e_1,\cdots,e_n$ of $V$ and consider the endomorphism $f\in\mathrm{GL}(V)$ defined by $f(e_i) = e_i + b\delta_{1,i}e_2$ for all $i$, where $b$ is a constant. We have $(\wedge^2 f)(e_1\wedge e_j) = e_1\wedge e_j + be_2\wedge e_j$ for all $j\geq 2$, and for $2\leq i<j$, $(\wedge^2 f)(e_i\wedge e_j) = e_i\wedge e_j$. Thus $\wedge^2 f$ is lower triangular in the basis of $e_i\wedge e_j$ with 1 on the diagonal, which gives $det(\wedge^2 f) = 1$.

Recall that any matrix of determinant 1 is a product of elementary matrices, hence by (ii) $\phi$ sends SL($V$) to SL($\wedge^2 V$). Take $t$ in an extension of $k$, such that $t^n det(f) = 1$. Then $det(tf) = 1$ and

$$1 = det(\wedge^2(tf)) = det(t^2 \wedge^2 f) = (t^2)^{\binom{n}{2}} det(\wedge^2 f),$$

which gives $det(\wedge^2 f) = t^{-n(n-1)} = det(f)^{n-1}$. □

**Solution to Problem 3.** We can change Z bases of $Z^5$ and $Z^3$ to turn $A$ in to a "canonical form". Equivalently, we can do the usual row-column reduction on $A$. Since $A$ rank 2 means that $AZ^3$ is a rank 2 subgroup of $Z^5$, which means the free part of $G$ is $Z^3$. So, in the reduced form $A$ has 3 zero rows, and 2 positive diagonal entries of all possibilities. We can arrange so that

$$G \simeq Z/a \oplus Z/b \oplus Z^3 \text{with } a \geq b > 0.$$

Finally list all possible non-isomorphic torsion part $Z/a \oplus Z/b$, by factorizing $a, b$.

Possible follow up: Generalize this as follows: $A$ is rank $k$ of size $m \times n$ with $m > n > k$. Classify all possible abelian groups of the form $G = \mathbb{Z}^m / A\mathbb{Z}^n$. The same method would likewise yield $G \simeq Z/a_1 \oplus \cdots \oplus Z/a_{n-k} \oplus Z^{m-k}$ with $a_1 \geq a_2 \geq \cdots \geq a_{n-k} > 0$. □