MAT 449 : Problem Set 6

Due Sunday, October 28

If G is a group, we say that a representation (π, V) of G is *faithful* if $\pi : G \to \mathbf{GL}(V)$ is injective.

1. Let $G = \mathbf{SU}(2)$. The group G acts on $\mathbb{C}^2$ via the inclusion $G \subset \mathbf{GL}_2(\mathbb{C})$, and we just denote this action by $(g, (z_1, z_2)) \mapsto g(z_1, z_2)$. (This is called the *standard representation* of G.)

   For every integer $n \geq 1$, let V_n be the space of polynomials $P \in \mathbb{C}[t_1, t_2]$ that are homogeneous of degree n (i.e. $P(t_1, t_2) = \sum_{r=0}^{n} a_r t_1^r t_2^{n-r}$, with $a_0, \ldots, a_n \in \mathbb{C}$).

   a) (3) If $P \in V_n$ and $g \in G$, show that the function $\mathbb{C}^2 \to \mathbb{C}$, $(z_1, z_2) \mapsto P(g^{-1}(z_1, z_2))$ is still given by a polynomial in V_n, and that this defines a continuous representation of G on V_n.

   b) (3) Show that the representation V_n of G is irreducible for every $n \geq 0$.

   c) (2) For which values of n is the representation V_n faithful ?

   Remark : We will see later that every irreducible unitary representation of $\mathbf{SU}(2)$ is isomorphic to one of the V_n.

   Solution.

   a) First take $P = t_1^r t_2^{n-r}$, with $0 \leq r \leq n$. Let $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SU}(2)$. As $\det(x) = 1$, we have $x^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. So

   $$P(x^{-1}(z_1, z_2)) = (dz_1 - bz_2)^r(-cz_1 + az_2)^{n-r}.$$

   This is still a homogeneous polynomial of degree n in z_1 and z_2, let's call it $P \circ x^{-1}$. Also, it is clear on the formula above that the map $G \to V_n$, $x \mapsto P \circ x^{-1}$ is continuous (which means that the coefficients of $P \circ x^{-1}$ are continuous functions of the entries of the matrix x).

   As the monomials $t_1^r t_2^{n-r}$, $0 \leq r \leq n$, generate V_n, the previous paragraph implies that, for every $P \in V_n$ and every $x \in \mathbf{SU}(2)$, the function $\mathbb{C}^2 \to \mathbb{C}$, $(z_1, z_2) \mapsto P(x^{-1}(z_1, z_2))$ is still given by an element of V_n, that we will denote by $P \circ x^{-1}$; it also implies that the map $G \to V_n$, $x \mapsto P \circ x^{-1}$ is continuous.

   For every $x \in G$, the map $V_n \to V_n$, $P \mapsto P \circ x^{-1}$ is clearly $\mathbb{C}$-linear in P. (In fact, we have already used that fact.) We also have $P \circ (xy)^{-1} = (P \circ y^{-1}) \circ x^{-1}$ for every $P \in V_n$ and all $x, y \in G$. So it follows from proposition I.3.5.1 of the notes that the map $G \times V_n \to V_n$, $(x, P) \mapsto P \circ x^{-1}$ is continuous, i.e. defines a continuous representation of G on V_n.

b) Let W be a G-invariant subspace of V. Let $P = \sum_{r=0}^{n} c_r t_1^r t_2^{n-r} \in W$. We show that, for every $r \in \{0, \dots, n\}$ such that $c_r \neq 0$, we have $t_1^r t_2^{n-r} \in W$. We prove this by induction on the number of nonzero coefficents of P. If P has 0 or 1 nonzero coefficients, we are done. Suppose that P has at least 2 nonzero coefficients. Fix $r \in \{0, \dots, n\}$ such that $c_r \neq 0$. It suffices to find another element Q of W such that the coefficient of $t_1^r t_2^{n-r}$ is nonzero, and such that Q has fewer nonzero coefficients than P; then we can apply the induction hypothesis to Q. Pick $s \in \{0, \dots, n\} - \{r\}$ such that $c_s \neq 0$. Consider $x_a = \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix}$, with $a \in S^1$. Then $x_a \in \mathbf{SU}(2)$, and

$$P \circ x_a^{-1} = \sum_{i=0}^{n} \overline{a}^i a^{n-i} c_i t_1^i t_2^{n-i} = \sum_{i=0}^{n} a^{n-2i} c_i t_1^i t_2^{n-i}.$$

Choose $a, a' \in S^1$ such that $a^{n-2s} c_s - (a')^{n-2s} c_s = 0$ and $a^{n-2r} c_r - (a')^{n-2r} c_r \neq 0$. Then $Q := P \circ x_a^{-1} - P \circ x_{a'}^{-1} \in W - \{0\}$ has the desired properties.

Now suppose that $W \neq 0$. By the previous paragraph, we can find $r \in \{0, \dots, n\}$ such that $P := t_1^t t_2^{n-r} \in W$. Let $x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$, with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. Then $x \in \mathbf{SU}(2)$ and $P \circ x^{-1} = (\overline{a} t_1 - b t_2)^r (\overline{b} t_1 + a t_2)^{n-r} \in W$. If we write $P \circ x^{-1} = \sum_{i=0}^{n} c_i t_1^i t_2^{n-i}$, then

$$c_i = \sum_{j=\max(0, i-n+r)}^{\min(i,r)} (-1)^{r-j} \binom{r}{j} \binom{n-r}{i-j} \overline{a}^j a^{n-r+j-i} b^{r-j} \overline{b}^{i-j}.$$

If we take $a = \frac{1}{\sqrt{1+t^2}}$ and $b = \frac{t}{\sqrt{1+t^2}}$ with $t \in [-1, 1]$, then each c_i is the quotient of a nonzero polynomial in t by $(1+t^2)^{n/2}$, so there are only finitely many values of t for which $c_i = 0$. Hence we can choose $x \in \mathbf{SU}(2)$ such that $P \circ x^{-1}$ has all its coefficients nonzero. By the first paragraph, this implies that every monomial $t_1^i t_2^{n-i}$, $0 \leq i \leq n$, is in W. So $W = V_n$.

c) Let's write π_n for the map $\mathbf{SU}(2) \to \mathbf{GL}(V_n)$. If $n = 0$, then V_n is the trivial representation of $\mathbf{SU}(2)$, so $\mathrm{Ker}(\pi_n) = \mathbf{SU}(2)$. Suppose that $n \geq 1$, and let $x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathrm{Ker}(\pi_n)$. In particular, if $P = t_1^n$, we must have $P \circ x^{-1} = P$. As $P \circ x^{-1} = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \overline{a}^i b^{n-i} t_1^i t_2^{n-i}$, this implies that $\overline{a}^n = 1$ and $\overline{a}^i b^{n-1} = 0$ for $0 \leq i \leq n-1$. In particular, $a \neq 0$, so we must have $b = 0$. Then $a \in S^1$, and, for every $r \in \{0, \dots, n\}$, $(t_1^r t_2^{n-r}) \circ x^{-1} = a^{n-2r} t_1^r t_2^{n-r}$, hence $a^{n-2r} = 1$. If n is odd, this implies that $a = 1$, so $x = I_2$ is the only element of $\mathrm{Ker}(\pi_n)$. If n is even, this only implies that $a = \pm 1$, so $x = \pm I_2$. In fact, if n is even and nonzero, it is easy to check that $-I_2$ acts trivially on V_n, so $\mathrm{Ker}(\pi_n) = \{\pm I_2\}$.

So to answer the question, the representation V_n is faithful if and only if n is odd.

□

2. Let (π, V) be a finite-dimensional unitary representation of $G := \mathbf{SL}_2(\mathbb{R})$. We want to show that V is trivial (i.e. $\pi(x) = \mathrm{id}_V$ for every $x \in G$).

a) (2) Consider the morphism of groups $\alpha : \mathbb{R} \to G$ sending $t \in \mathbb{R}$ to the matrix $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

Show that there exist a basis $\mathcal{B}$ of V and $y_1, \dots, y_n \in \mathbb{R}$, where $n = \dim V$, such that, for every $t \in \mathbb{R}$, the endormophism $\pi(\alpha(t))$ is diagonal in $\mathcal{B}$ with diagonal entries $e^{ity_1}, \dots, e^{ity_n}$.

b) (3) Show that $\pi(\alpha(t)) = \mathrm{id}_V$ for every $t \in \mathbb{R}$. (Hint : If $u \in \mathbb{R}^\times$ and $x = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$, consider the action of $x\alpha(t)x^{-1}$ on V.)

c) (2) Show that $\pi(x) = \mathrm{id}_V$ for every $x \in G$.

d) (2, extra credit) If $n \geq 3$, show that every finite-dimensional unitary representation of $\mathbf{SL}_n(\mathbb{R})$ is trivial.

Solution.

a) The subgroup $\pi(\alpha(\mathbb{R}))$ of $\mathbf{GL}(V)$ is commutative, and all its elements are diagonalizable (because they are all unitary), so we can find a basis $\mathcal{B} = (v_1, \ldots, v_n)$ of V in which all the elements of $\pi(\alpha(\mathbb{R}))$ are diagonal, and even an orthonormal basis if we want. (If you don't like simultaneously diagonalizing an infinite subset of $\mathbf{GL}(V)$, just choose $A_1, \ldots, A_m \in \pi(\alpha(\mathbb{R}))$ that generate $\mathrm{Span}(\pi(\alpha(\mathbb{R})))$ and simultanesouly diagonalize them.)

For every $j \in \{1, \ldots, n\}$, the subspace $\mathbb{C}v_j$ is stable by the action of $\alpha(\mathbb{R}) \subset G$ (by the choice of the basis), so we get a 1-dimensional representation of $\mathbb{R}$ on $\mathbb{C}v_j$, and we know by 5(b) of problem set 3 that such a representation is of the form $t \mapsto e^{ity_j}v_j$, for a $y_j \in \mathbb{C}$.

b) We have $x\alpha(t)x^{-1} = \alpha(u^2t)$, so $\pi(x\alpha(t)x^{-1})$ is diagonal in the basis $\mathcal{B}$ with diagonal entries $e^{iu^2ty_1}, \ldots, e^{iu^2ty_n}$. On the other hand, we have $\mathrm{Tr}(\pi(x\alpha(t)x^{-1})) = \mathrm{Tr}(\pi(x)\pi(\alpha(t))\pi(x)^{-1}) = \mathrm{Tr}(\pi(\alpha(t))$, hence, for every $t \in \mathbb{R}$ and every $u \in \mathbb{R}^\times$,

$$\sum_{j=1}^{n} e^{ity_j} = \sum_{j=1}^{n} e^{iu^2ty_j}.$$

Suppose that we know that the subset $\widehat{\mathbb{R}}$ of $L^\infty(\mathbb{R})$ is linearly independent. Then the equality tells us that, for every $u \in \mathbb{R}^\times$, the sets $\{y_1, \ldots, y_n\}$ and $\{u^2y_1, \ldots, u^2y_n\}$ are equal. This is only possible if $y_1 = \ldots = y_n = 0$, which in turn implies that $\alpha(t)$ acts trivially on V for every $t \in \mathbb{R}$.

Now let's show the statement about $\widehat{\mathbb{R}}$. Let $y_1, \ldots, y_m \in \mathbb{R}$ be pairwise distinct and $c_1, \ldots, c_m \in \mathbb{C}$ be such that $\sum_{j=1}^m c_j e^{ity_j} = 0$ for every $t \in \mathbb{R}$. We want to show that $c_1 = \ldots = c_m = 0$. Let $r \in \mathbb{R}$. Taking $t = 0, r, \ldots, r(m-1)$, and using the calculation of the Vandermonde determinant, we see that we must have $e^{iry_1} = \ldots = e^{iry_m}$. As this is true for every $r \in \mathbb{R}$, it implies that $y_1 = \ldots = y_m$ (for example by taking the derivative with respect to r of the previous equalities and then evaluating at $r = 0$). So $m = 1$, and then the fact that $c_1 e^{ity_1} = 0$ for every $t \in \mathbb{R}$ implies that $c_1 = 0$.

c) If $x \in \mathbf{SL}_2(\mathbb{R})$ is a transvection (aka shear) matrix, then we have $x = y\alpha(t)y^{-1}$ for some $t \in \mathbb{R}$ and some $y \in \mathbf{SL}_2(\mathbb{R})$, so $\pi(x) = \pi(y)\pi(\alpha(t))\pi(y)^1 = \pi(y)\pi(y)^{-1} = \mathrm{id}_V$ by (b). As $\mathbf{SL}_2(\mathbb{R})$ is generated by transvection matrices, this implies that $\pi(x) = \mathrm{id}_V$ for every $x \in \mathbf{SL}_2(\mathbb{R})$.

d) Let $\pi : \mathbf{SL}_n(\mathbb{R}) \to \mathbf{GL}(V)$ be a finite-dimensional unitary representation. Let $x \in \mathbf{SL}_n(\mathbb{R})$ be a transvection matrix. We could imitate (a) and (b) to prove that $\pi(x) = \mathrm{id}_V$, but we can also do the following thing : Choose a basis $(v_1, \ldots, v_n)$ of $\mathbb{R}^n$ in which the matrix of the linear endomrophism of $\mathbb{R}^n$ corresponding to x is $\begin{pmatrix} 1 & 1 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & \ldots & 0 & \ddots & 0 \\ 0 & & \ldots & & 1 \end{pmatrix}$. Consider the subset G of $\mathbf{SL}_n(\mathbb{R})$ composed of the elements

whose matrix in $(v_1, \ldots, v_n)$ is of the form $\begin{pmatrix} a & b & 0 & \ldots & 0 \\ c & d & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & \ldots & 0 & \ddots & 0 \\ 0 & & \ldots & & 1 \end{pmatrix}$, with $a, b, c, d \in \mathbb{R}$ and $ad - bc = 1$. Then G is a subgroup, and it is isomorphic to $\mathbf{SL}_2(\mathbb{R})$. As $\pi_{|G}$ is a unitary representation of G on V, we have $G \subset \mathrm{Ker}(\pi)$ by (c). In particular, $\pi(x) = \mathrm{id}_V$.

Now we use the fact that $\mathbf{SL}_n(\mathbb{R})$ is generated by transvections matrices to conclude that $\pi(x) = \mathrm{id}_V$ for every $x \in \mathbf{SL}_n(\mathbb{R})$.

□

The preceding problem shows that $\mathbf{SL}_2(\mathbb{R})$ has no faithful finite-dimensional unitary representation. But at least $\mathbf{SL}_2(\mathbb{R})$ has faithful continuous finite-dimensional representations, for example the one given by the inclusion $\mathbf{SL}_2(\mathbb{R}) \subset \mathbf{GL}_2(\mathbb{C})$.

We can also ask if there exist locally compact groups that don't have faithful irreducible unitary representations at all. The answer is "yes".

3. (3) Show that, if (π, V) is an irreducible unitary representation of $\mathbf{GL}_n(\mathbb{Z}_p)$, then there exists $m \geq 1$ such that $\pi(I_n + p^m M_n(\mathbb{Z}_p)) = \{1\}$.

   Solution. By 4(m) of problem set 1, the group $\mathbf{GL}_n(\mathbb{Z}_p)$ is compact. Hence, by problem 6 of problem set 5, the space V is finite-dimensional. Now the proof of the statement is exactly as in 3(c) of problem set 3.

   □

4. (extra credit, 3) More generally, show that, if G is a profinite group (i.e. a projective limit of finite discrete groups, see problem 3 of problem set 1), then G has a faithful irreducible unitary representation only if G is finite.

Solution. We know that G is compact Hausdorff by problem 3 of problem set 1 (note that finite discrete groups are comact Hausdorff). So, by problem 6 of problem set 5, every irreducible unitary representation of G is finite-dimensional.

Suppose that we know that G is totally disconnected. Let (π, V) be a continuous finite-dimensional representation of G. By 2(c) of problem set 3, the compact open subgroups of G form a basis of neighborhoods of 1. By 3(b) of the same problem set, we can find a neighborhood U of id_v in $\mathbf{GL}(V)$ such that the only subgroup of $\mathbf{GL}(V)$ contained in U is $\{\mathrm{id}_V\}$. So, if we choose a compact open subgroup K of G such that $\pi(K) \subset U$, we must have $K \subset \mathrm{Ker}(\pi)$. Hence $\mathrm{Ker}(\pi) = \bigcup_{x \in \mathrm{Ker}(\pi)} xK$ is an open subgroup of G, and so the group $G/\mathrm{Ker}(\pi)$ is discrete. As it is also compact, it is a finite group. This shows that G cannot have a faithful irreducible unitary representation unless it is finite.

So it remains to show that G is totally disconnected, i.e. that the only nonempty connected subsets of G are the singletons. Take a projective system $((G_i)_{i \in I}, (u_{ij} : G_i \to G_j)_{i \geq j})$ of finite groups such that $G = \varprojlim_{i \in I} G_i$. Let $C \subset G$ be a nonempty connected subset. Then the image of G in each G_i is connected nonempty, hence a singleton $\{g_i\}$. This implies that the only element of C is the family $(g_i)_{i \in I} \in \prod_{i \in I} G_i$ (this family is automatically in the projective limit).

Remark : It is not true that a finite group always has a faithful irreducible unitary representation. For example, if G is a finite abelian group, then every irreducible unitary representation of G is 1-dimensional by Schur's lemma. Take $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and let $\pi : G \to \mathbb{C}$ be a 1-dimensional representation. As (1.0) and $(0,1)$ are of order 2 in G, we must have $\pi(1,0), \pi(0,1) \in \{\pm 1\}$. If we want π to be faithful, we need to have $\pi(1,0) = \pi(0,1) = -1$, but then $\pi(1,1) = (-1)^2 = 1$, so π cannot be faithful. (More generally, a finite abelian has a faithful 1-dimensional representation if and only if it is cyclic.)

□

We will now see how to find discrete groups that have no faithful finite-dimensional representations at all, over any field.

Let Γ be a (discrete) group. We say that Γ is *residually finite* if, for every $x \in \Gamma - \{1\}$, there exists a normal subgroup Δ of Γ such that Γ/Δ is finite (we say that Δ is of *finite index* in Γ) and that the image of x in Γ/Δ is not trivial.

The goal of the following two problems is to prove that, if k is a field and $\Gamma \subset \mathbf{GL}_n(k)$ is a finitely generated subgroup, then Γ is residually finite. [1]

5. Let R be a finitely generated $\mathbb{Z}$-algebra that is also a domain. We fix an integer $n \geq 1$. For every ideal I of R, we set

$$\Gamma(I) = \mathrm{Ker}(\mathbf{GL}_n(R) \to \mathbf{GL}_n(R/I)).$$

   a) (3) Show that R is a field if and only if R is finite.

   b) (2) If $\mathfrak{m}$ is a maximal ideal of R, show that $\Gamma(\mathfrak{m})$ is a normal subgroup of finite index in $\mathbf{GL}_n(R)$.

   c) (3) Show that the intersection of all the maximal ideals of R is 0. (Hint : We may assume that R is not a field. If $a \in R - \{0\}$, show that the localization $R[1/a]$ is not a field, take a maximal ideal in $R[1/a]$, and intersect it with R.)

   d) (1) Show that $\mathbf{GL}_n(R)$ is residually finite.

Solution.

a) It's a classical fact that a finite integral domain has to be a field. Here is the proof. Suppose that R is finite, and let $a \in R - \{0\}$. Then multiplication by a is an additive map from R to itself, and its kernel is $\{0\}$ (because R is an integral domain), so it is injective; as R is finite, it is also surjective, which means that there exists $b \in R$ such that $ab = 1$, i.e. that $a \in R^\times$.

The converse follows from two classical results of commutative algebra (see for example exercises 4.30 and 4.32 of Eisenbud's *Commutative algebra*) :

- If $K \subset L$ is a field extension such that L is finitely generated as a K-algebra, then L is a finite-dimensional K-vector space (Zariski's lemma).
- If R is a Noetherian ring, S is a finitely generated R-algebra and $T \subset S$ is a R-subalgebra such that S is a finite T-algebra (i.e. finitely generated as a T-module), then T is a finitely generated R-algebra (Artin-Tate).

Indeed, if R is a field, consider its prime field k. Then R is a finitely generated k-algebra, hence a finite dimension k-vector space by Zariski's lemma, which implies that k is a finitely generated $\mathbb{Z}$-algebra by the second result. Note that k is either

[1] In fact, we can use similar ideas to show that, if $\mathrm{char}(k) = 0$, such a Γ has to be virtually residually p-finite (i.e. it has a finite index subgroup Γ' such that, for every $x \in \Gamma' - \{1\}$, there exists a finite index normal subgroup $\Delta \not\ni x$ of Γ' such that Γ'/Δ is a p-group) for almost every prime number p, but the only proof I know uses the Noether normalization theorem.

$\mathbb{Q}$ or one of the finite fields $\mathbb{F}_p$. But $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra (if $x_1, \ldots, x_n \in \mathbb{Q} - \{0\}$, and if $\mathcal{P}$ is the (finite) set of prime numbers that divide the denominator of one of the x_i, then the prime numbers dividing the denominator of a nonzero element of the $\mathbb{Z}$-subalgebra generated by $x_1, \ldots, x_n$ has to also be in $\mathcal{P}$, so this $\mathbb{Z}$-subalgebra cannot be equal to $\mathbb{Q}$). So k is a finite field; as R is a finite-dimensional k-vector space, it is also a finite field.

For completeness, let's give a proof of the part of the commutative algebra results that we actually need. Suppose that we know the following :
(*) Let L/K be a field extension such that :

- there exists $u \in L$ such that $L = K(u)$ (i.e. L is generated by u as a field);
- L is a finitely generated $\mathbb{Z}$-algebra,

the extension is finite and K is also a finitely generated $\mathbb{Z}$-algebra.

Then we can prove in the same way that, if R is a field, it has to be finite. (Just choose elements $x_1, \ldots, x_n \in R$ generating R over its prime field k and apply (*) to the extensions $k(x_1, \ldots, x_{i-1}) \subset k(x_1, \ldots, x_i)$ to show that k is a finitely generated $\mathbb{Z}$-algebra. The end of the proof is as before.)

We now prove (*). Let $x_1, \ldots, x_n \in L^\times$ generating L as a $\mathbb{Z}$-algebra. Assume that u is transcendental over K; then L is isomorphic to the field of rational fractions of K. Write $x_i = \frac{P_i}{Q_i}$, with $P_i, Q_i \in K[u]$. As $(1 + u\prod_{i=1}^n Q_i)^{-1} = L = \mathbb{Z}[a_1, \ldots, a_n]$, we can write

$$(1 + u\prod_{i=1}^{n} Q_i)^{-1} = \frac{R}{Q_1^{d_1} \ldots Q_n^{d_n}},$$

with $R \in K[u]$ coprime to all the Q_i and $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 0}$. We get $Q_1^{d_1} \ldots Q_n^{d_n} = R(1 + u\prod_{i=1}^n Q_i)$, which contradicts the fact that R is coprime to all the Q_i. So u is algebraic over K. Let $X^d + a_1 X^{d-1} + \ldots + a_d \in K[X]$ be the minimal polynomial of u over K. For every $i \in \{1, \ldots, n\}$, write $x_i = \sum_{j=0}^{d-1} b_{ij} u^j$, with $b_{ij} \in K$. Let A be the $\mathbb{Z}$-algebra of K generated by $a_1, \ldots, a_d$ and by the b_{ij}, and let's show that $A = K$. Let $y \in K$. Then y can be written as a polynomial in $x_1, \ldots, x_d$ with coefficients in $\mathbb{Z}$, so it is also a polynomial in u with coefficients in A, which can be taken of degree $\leq d - 1$ (we can use the relation $u^d = -a_1 u^{d-1} - \ldots - a_d$ to replace any terms of degree $\geq d$ with terms of lower degree). In other words, we can write $y = \sum_{i=0}^{d-1} c_i u^i$, with $c_0, \ldots, c_{d-1} \in A$. As the family $(1, u, \ldots, u^{d-1})$ is linearly independent over K, we must have $c_1 = \ldots = c_{d-1} = 0$ and $y = c_0 \in A$.

b) First, the group $\Gamma(I)$ is a normal subgroup of $\mathbf{GL}_n(R)$ for any ideal, because it is the kernel of a morphism of groups. Suppose that $\mathfrak{m}$ is a maximal ideal. Then $R/\mathfrak{m}$ is a finite field by (a). As $\mathbf{GL}_n(R)/\Gamma(\mathfrak{m})$ injects into $\mathbf{GL}_n(R/\mathfrak{m})$, this implies that $\Gamma(\mathfrak{m})$ has finite index in $\mathbf{GL}_n(R)$.

c) If R is a field, then (0) is a maximal ideal of R and we are done. Suppose that R is not a field; in particular, by (a), it is not finite. Let $a \in R - \{0\}$. The localization $R[1/a] := R[X]/(aX - 1)$ is a finitely generated $\mathbb{Z}$-algebra because R is, so it can only be a field if it is finite, by (a). But the obvious map $R \to R[1/a]$ is injective because a is not a divisor of 0 (remember that R is an integral domain), and R is infinite, so $R[1/a]$ is also infinite, hence it is not a field. Let $\mathfrak{m}'$ be a maximal ideal of $R[1/a]$, and let $\mathfrak{m}$ be its inverse image in R. Then the map $R/\mathfrak{m} \to R[1/a]/\mathfrak{m}'$ is injective (because $R \to R[1/a]$ is), and $R[1/a]/\mathfrak{m}'$ is finite because it is a field (by (a)), so $R/\mathfrak{m}$ is finite and an integral domain, so it is a field (by (a) again !), and $\mathfrak{m}$ is a maximal ideal of R. Note also that, as a is invertible in $R[1/a]$, it cannot be in $\mathfrak{m}'$, and so it cannot be in $\mathfrak{m}$. So we have found a maximal ideal of R that doesn't contain a.

d) Let $x = (x_{ij})_{1 \leq i,j \leq n} \in \mathbf{GL}_n(R)$ such that $x \neq I_n$. Choose $i, j \in \{1, \ldots, n\}$ such that $x_{ij} \neq 0$ and $i \neq j$, or such that $x_{ij} \neq 1$ and $i = j$. By (c), we can find a maximal ideal $\mathfrak{m}$ of R such that $x_{ij} \notin \mathfrak{m}$ if $i \neq j$, and such that $x_{ij} - 1 \notin \mathfrak{m}$ if $i = j$. In other words, the image of x in $\mathbf{GL}_n(R)/\Gamma(\mathfrak{m})$ is not the unit element. As $\Gamma(\mathfrak{m})$ is a normal subgroup of $\mathbf{GL}_n(R)$ of finite index by (b), we are done.

□

6. Let k be a field, and let Γ be a finitely generated subgroup of $\mathbf{GL}_n(k)$.

   a) (2) Show that there exists a finitely generated $\mathbb{Z}$-subalgebra R of k such that $\Gamma \subset \mathbf{GL}_n(R)$.

   b) (1) Show that Γ is residually finite.

   Solution.

   a) Let $\gamma_1, \ldots, \gamma_n$ be generators of Γ, and let R be the $\mathbb{Z}$-subalgebra of k generated by the entries of the γ_i and of their inverses; this is a finitely generated $\mathbb{Z}$-algebra by definition. As each element of Γ is a product of the elements $\gamma_i^{\pm 1}$, we have $\Gamma \subset \mathbf{GL}_n(R)$.

   b) This follows immediately from 5(d) : If $\gamma \in \Gamma - \{1\}$, choose a normal subgroup of finite index Δ of $\mathbf{GL}_n(R)$ such that the image of γ in $\mathbf{GL}_n(R)/\Delta$ is not trivial. Then $\Gamma \cap \Delta$ is a normal subgroup of Γ, and $\Gamma/(\Gamma \cap \Delta)$ injects into $\mathbf{GL}_n(R)/\Delta$, so $\Gamma \cap \Delta$ is of finite index in Γ and the image of γ in $\Gamma/(\Gamma \cap \Delta)$ is not trivial.

   □

Of course, the result of the previous problem would not be very interesting if we could not give any example of a finitely generated non residually finite group. So let's do that.

7. Let Γ be the quotient of the free group on the generators a and b by the relation $a^{-1}b^2a = b^3$. In this problem, we will assume that $b_1 := a^{-1}ba$ and b do not commute in Γ, and deduce that Γ is not residually finite.

   Let $u : \Gamma \to \Gamma'$ be a morphism of groups, with Γ' finite.

   a) (2) Let n be the order of $u(a)$ in Γ'. Show that the order of $u(b)$ divides $3^n - 2^n$.

   b) (2) Show that there exists an integer $N \geq 0$ such that $u(b_1) = u(b_1^2)^N$. (Note that the order of $u(b)$ is prime to both 2 and 3.)

   c) (1) Show that $u(b_1)$ and $u(b)$ commute.

   d) (1) Show that Γ is not residually finite.

   Solution.

   a) We first prove that, for every $r \in \mathbb{Z}_{\geq 0}$, we have $b^{2^r} = a^r b^{3^r} a^{-r}$. The case $r = 0$ is obvious, and the case $r = 1$ is the relation defining Γ. Let $r \geq 1$, suppose the result know for r, and let's prove it for $r + 1$. We have

   $$b^{2^{r+1}} = (b^2)^{2^r} = (ab^3a^{-1})^{2^r} = (ab^{2^r}a^{-1})^3 = (a^{r+1}b^{3^r}a^{-(r+1)})^3 = a^{r+1}b^{3^{r+1}}a^{-(r+1)}.$$

   Applying to $r = n$ gives $b^{2^n} = a^n b^{3^n} a^{-n}$, hence $u(b)^{3^n - 2^n} = 1$, so the order of $u(b)$ divides $3^n - 2^n$.

b) Note that the order of $u(b)$ is odd, because it divides the odd number $3^n - 2^n$. So there exists $N \geq 1$ such that $u(b)^{2N} = u(b)$. As $b_1 = a^{-1}ba$, we have $b_1^r = a^{-1}b^r a$ for every $r \geq 0$, so $u(b_1)^{2N} = u(b_1)$, as desired.

c) We have $b_1^2 = b^3$ by the relation defining, so $u(b_1) = u(b)^{3N}$ by (b). This implies that $u(b)$ and $u(b_1)$ commute.

d) Let $c = b_1^{-1}b^{-1}b_1 b \in \Gamma$. Then we have assumed that $c \neq 1$, but question (c) shows that, for every normal subgroup of finite index Δ of Γ, the image of c in Γ/Δ is trivial. So Γ is not residually finite.

□

8. (extra credit) Let Γ be the quotient of the free group on the generators a and b by the relation $a^{-1}b^2a = b^3$. The goal of this problem is to show that $b_1 := a^{-1}ba$ and b do not commute in Γ, i.e. that $b_1 b b_1^{-1} b^{-1}$ is not trivial in Γ. [2]

Let F be the free group on the generators a and b. Remember that elements of F are reduced words in the letters a, a^{-1}, b, b^{-1}. (A reduced words is a word that contains no redundant pair aa^{-1}, $a^{-1}a$, bb^{-1} or $b^{-1}b$.) We write an element of F as $a^{n_1}b^{m_1}\dots a^{n_r}b^{m_r}$, with $n_1, m_1, \dots, n_r, m_r \in \mathbb{Z}$ and $m_1, n_2, m_2, \dots, n_{r-1}, m_{r-1}, n_r \neq 0$.

Let Ω be the set of reduced words of the form $b^{r_1}a^{s_1}\dots b^{r_m}a^{s_m}b^r$, with :

(i) $m \in \mathbb{Z}_{\geq 0}$ and $r_i, s_i, r \in \mathbb{Z}$;

(ii) $s_i \neq 0$ for every $i \in \{1, \dots, m\}$;

(iii) $r_i \neq 0$ for every $i \in \{2, \dots, m\}$;

(iv) for every $i \in \{1, \dots, m\}$, if $s_i > 0$, then $0 \leq r_i \leq 1$;

(v) for every $i \in \{1, \dots, m\}$, if $s_i < 0$, then $0 \leq r_i \leq 2$.

By definition of Γ, we have a surjective group morphism $F \to \Gamma$, that we will denote by φ.

a) (2) Show that $\varphi(\Omega) = \Gamma$.

b) (1) For every $w \in \Omega$ and every $s \in \{a, a^{-1}, b, b^{-1}\}$, find a word $w' \in \Omega$ such that $\varphi(w') = \varphi(ws)$. We will denote this w' by $w \cdot s$ in what follows.

c) (1) For every $w \in \Omega$ and every $s \in \{a, a^{-1}, b, b^{-1}\}$, show that $(w \cdot s) \cdot s^{-1} = w$.

d) (1) Show that $(w, s) \mapsto w \cdot s$ extends to a right action of Γ on Ω.

e) (1) Show that φ induces a bijection $\Omega \xrightarrow{\sim} \Gamma$.

f) (1) Show that $b_1 b b_1^{-1} b^{-1} \neq 1$ in Γ.

Solution.

a) By definition of the free group, we can write every element w of F as a reduced word $b^{r_1}a^{s_1}\dots b^{r_m}a^{s_m}b^r$ satisfying conditions (i), (ii) and (iii). We define $N(w)$ to be the max of all $s_i > 0$ such that $r_i \notin \{0, 1\}$; so if w satisfies condition (iv), we have $N(w) = 0$. We define $M(w)$ to be the max of all $|s_i|$, for $s_i < 0$ such that $r_i \notin \{0, 1, 2\}$; so if w satisfies condition (v), we have $M(w) = 0$. We prove by induction on $N(w) + M(w)$ that there exists $w_0 \in \Omega$ such that $\varphi(w) = \varphi(w_0)$. If $N(w) + M(w) = 0$, then w satisfies conditions (iv) and (v), so it is in Ω and the conclusion is obvious.

[2] The easiest way to show this would to find a finite-dimensional representation of Γ on which $b_1 b b_1^{-1} b$ acts non-trivially, but we can't. Still, some variant of this idea will work.

Suppose that $N(w) + M(w) > 0$. If $N(w) > 0$, choose $i \in \{1, \dots, m\}$ such that $s_i > 0$ and $r_i \notin \{0, 1\}$. Note that the relation defining Γ says that $\varphi(b^2 a) = \varphi(ab^3)$, hence also that $\varphi(b^{-2}a) = \varphi(ab^{-3})$, which implies that $\varphi(b^{2k}a) = \varphi(ab^{3k})$ for every $k \in \mathbb{Z}$. Write $r_i = 2k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1\}$, and let

$$w' = b^{r_1} a^{s_1} \dots b^{r_{i-1}} a^{s_{i-1}} b^l a b^{3k} a^{s_i - 1} b^{r_{i+1}} a^{s_{i+1}} \dots b^{r_m} a^{s_m} b^r.$$

Then $\varphi(w) = \varphi(w')$ by the observation above, and $N(w') < N(w)$, $M(w') = M(w)$. Similarly, if $M(w) > 0$, choose $i \in \{1, \dots, m\}$ such that $s_i < 0$ and $r_i \notin \{0, 1, 2\}$. For $k \in \mathbb{Z}$, the equality $\varphi(b^{2k}a) = \varphi(ab^{3k})$ can also be written $\varphi(a^{-1}b^{2k}) = \varphi(b^{3k}a^{-1})$. Write $r_i = 3k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$, and let

$$w' = b^{r_1} a^{s_1} \dots b^{r_{i-1}} a^{s_{i-1}} b^l a^{-1} b^{2k} a^{s_i + 1} b^{r_{i+1}} a^{s_{i+1}} \dots b^{r_m} a^{s_m} b^r.$$

Then $\varphi(w) = \varphi(w')$ by the observation above, and $N(w') = N(w)$, $M(w') < M(w)$. As one of $N(w)$ or $M(w)$ has to be > 0, we can always find $w' \in F$ such that $\varphi(w') = \varphi(w)$ and $N(w') + M(w') < N(w) + M(w)$. Applying the induction hypothesis to w' gives the result.

b) Let $w = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^r \in \Omega$; we assume that conditions (i)-(v) are satisfied. If $s = b$ (resp. $s = b^{-1}$), then $w' = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^{r+1}$ (resp. $w' = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^{r-1}$) works. If $s = a$, write $r = 2k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1\}$ and take $w' = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a b^{3k}$. If $s = a^{-1}$, write $r = 3k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$ and take $w' = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a^{-1} b^{2k}$.

c) The conclusion is obvious if $s \in \{b, b^{-1}\}$. Suppose that $s = a$ and write $r = 2k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1\}$. Then $w \cdot a = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a b^{3k}$, so

$$(w \cdot a) \cdot a^{-1} = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a a^{-1} b^{2k} = w.$$

If $s = a^{-1}$, write $r = 3k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$. Then $w \cdot a = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a^{-1} b^{2k}$, so

$$(w \cdot a^{-1}) \cdot a = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a^{-1} a b^{3k} = w.$$

d) By (c), $(w, s) \mapsto w \cdot s$ extends to a right action of F on Ω. To prove that this factors through a right action of Γ on Ω, it suffices to show that $b^{-3}a^{-1}b^2 a$ acts trivially. Let $w = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^r \in \Omega$; we assume that conditions (i)-(v) are satisfied. Write $r = 3k + l$, with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$. Then

$$w \cdot b^{-3} = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^{r-3} = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^{l+3(k-1)},$$

so

$$w \cdot (b^{-3} a^{-1}) = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a^{-1} b^{2(k-1)},$$

hence

$$w \cdot (b^{-3} a^{-1} b^2) = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a^{-1} b^{2k},$$

and finally

$$w \cdot (b^{-3} a^{-1} b^2 a) = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^l a^{-1} a b^{3k} = b^{r_1} a^{s_1} \dots b^{r_m} a^{s_m} b^{l+3k} = w.$$

e) We already know that $\varphi(\Omega) = \Gamma$ by (a), so we just need to show that $\varphi_{|\Omega}$ is injective. By the explicit formulas for the action given in the proof of (b), if $w \in \Omega$, then we have $1 \cdot w = w$. As $1 \cdot w$ only depends on $\varphi(w)$ by (d), this shows that $\varphi(w)$ determines w.

f) By (e), we just need to show that the unique preimage of $\varphi(b_1 b b_1^{-1} b^{-1})$ in Ω is not trivial. We have seen in the proof of (a) an algorithm to transform a reduced word into an element of Ω having the same image by φ. Applying it to $b_1 b b_1^{-1} b^{-1} = a^{-1}baba^{-1}b^{-1}ab^{-1}$, we get $a^{-1}baba^{-1}bab^{-4} \neq 1$ (modulo easy-to-make mistakes), so we are done.

□