# ALGEBRA II: SOLUTIONS

**Problem 1.** Let $k$ be a positive integer. The group $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ consists of matrices with entries in the ring $\mathbb{Z}/2^k\mathbb{Z}$ whose determinant is a unit of $\mathbb{Z}/2^k\mathbb{Z}$. Show that $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is a solvable group. You may use without proof that $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ is solvable.

**Solution.** Let $G_k = \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$. We show that $G_k$ is solvable by induction on $k$. The base case $k = 1$ is given to us. Now let $k > 1$. We can take an element of $G_k$ and reduce its entries modulo $2^{k-1}$ to obtain an element of $G_{k-1}$. This defines a group homomorphism $\pi_k \colon G_k \to G_{k-1}$. Since $G_{k-1}$ is solvable by assumption, it is enough to show that $\ker(\pi_k)$ is solvable, as this will imply that $G_k$ is solvable.

The kernel of $\pi_k$ consists of all matrices in $G_k$ that are congruent to the identity matrix modulo $2^{k-1}$. Such matrices have the form $1 + 2^{k-1}A$ where $A$ is some $2 \times 2$ matrix with entries in $\mathbb{Z}/2^k\mathbb{Z}$ and 1 is the identity matrix; in fact, every matrix of this form is invertible and thus belongs to $\ker(\pi_k)$, but this is not needed. We have

$$(1 + 2^{k-1}A)(1 + 2^{k-1}B) = 1 + 2^{k-1}(A + B) + 2^{2k-2}AB \equiv 1 + 2^{k-1}(A + B) \pmod{2^k}.$$

Reversing the order gives a similar computation, and so we see that

$$(1 + 2^{k-1}A)(1 + 2^{k-1}B) \equiv (1 + 2^{k-1}B)(1 + 2^{k-1}A) \pmod{2^k}.$$

It follows that $\ker(\pi_k)$ is commutative, and in particular solvable.

**Problem 2.** Let $G$ be a group with the following presentation:

$$G = \left\langle a, b \;\middle|\; (a^2b)^5 = 1,\ a^2ba^{-1}b^{-2} \right\rangle$$

and let $[G, G]$ be the commutator subgroup of $G$. Compute the order of the quotient $G/[G, G]$.

**Solution.** Recall that $G/[G, G]$ is called the abelianization of $G$ and denoted $G_{\mathrm{ab}}$. The abelianization of the free group $F = \langle a, b\rangle$ is $\mathbb{Z}^2$; let $\overline{a}$ and $\overline{b}$ be the images of $a$ and $b$, which are generators of $F_{\mathrm{ab}}$. The image of $(a^2b)^5$ in $F_{\mathrm{ab}}$ is $10\overline{a} + 5\overline{b}$, while the image of $a^2ba^{-1}b^{-2}$ is $\overline{a} - \overline{b}$. We thus have an isomorphism

$$G_{\mathrm{ab}} = (\mathbb{Z}\overline{a} \oplus \mathbb{Z}\overline{b})/(10\overline{a} + 5\overline{b}, \overline{a} - \overline{b}).$$

In other words, $G_{\mathrm{ab}}$ has presentation matrix

$$\begin{pmatrix} 10 & 1 \\ 5 & -1 \end{pmatrix}.$$

The cardinality of $G_{\mathrm{ab}}$ is the absolute value of the determinant of this matrix, i.e., 15.

**Problem 3.** Let $L/F$ be a field extension and let $K_1$ and $K_2$ be two distinct subfields with $F \subset K_1, K_2 \subset L$ such that $L = K_1K_2$ and $[K_1 : F] = [K_2 : F] = 3$. Show that $[L : F]$ is either 6 or 9, and give examples to show that both values can occur.

*Date*: August 2022.

**Solution.** Let $x$, $y$, $z$ be an $F$-basis for $K_2$. Since $L = K_1K_2$, we see that $x$, $y$, $z$ is a $K_1$-spanning set for $L$, so $[L : K_1] \leq 3$. Also, since $K_1 \neq K_2$, we have $L \neq K_1$, so $[L : K_1] \geq 1$. Thus, $[L : K_1]$ is 2 or 3 and $[L : F] = [L : K_1][K_1 : F] = [L : K_1] \cdot 3$ is either 6 or 9.

To see that the value 6 can occur, take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt[3]{2})$, $K_2 = \mathbb{Q}(\omega\sqrt[3]{2})$ and $L = \mathbb{Q}(\omega, \sqrt[3]{2})$, where $\omega$ is a primitive cube root of unity. To see that the value 9 can occur, take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt[3]{2})$, $K_2 = \mathbb{Q}(\sqrt[3]{3})$ and $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.

**Problem 4.** Let $L$ be the field $\mathbb{C}(x_1, x_2, x_3, x_4)$ of rational functions in four independent variables. Let $K \subset L$ be the subfield of $S_4$-symmetric functions. Give an explicit element $\theta \in L$ such that $[K(\theta) : K] = 3$.

**Solution.** The extension $L/K$ is a Galois extension with Galois group $S_4$. So an extension $K(\theta)$ with $[K(\theta) : K] = 3$ corresponds to an index 3 subgroup of $S_4$, in other words, a subgroup $H$ of $S_4$ of order 8. The subgroups of $S_4$ of order 8 are the dihedral group $D := \langle (1234), (13) \rangle$ and its conjugates. So $[L^D : K] = 3$ for this group $D$. Since 3 is prime, if $\theta$ is any element of $L^D$ not in $K$, then $L^D = K(\theta)$. Such a $\theta$ is $x_1x_3 + x_2x_4$.

**Problem 5.** Let $G$ be a group of order $4n$ with $n$ odd. Suppose that $G$ contains (at least) two distinct cyclic groups of order $2n$. Show that $G$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/n\mathbb{Z})$.

**Solution.** Let $N_1 \neq N_2$ be two cyclic subgroups of order $2n$. Observe the following:

- $N_1$ and $N_2$ are normal in $G$, since they have index 2.
- $G = N_1N_2$; indeed, since $N_2$ is normal $N_1N_2$ is the subgroup generated by $N_1$ and $N_2$, and this is strictly larger than $N_2$, and thus all of $G$ since $N_2$ already has index 2.
- $Z = N_1 \cap N_2$ is cyclic of order $n$; indeed, it is a subgroup of $N_1$, and therefore cyclic, and has index 2 in $N_1$ (since $N_2$ has index 2 in $G$), and thus has order $n$.

Now, $Z$ is obviously central in each of $N_1$ and $N_2$. By the second point above, it follows that $Z$ is central in $G$.

Now, $N_1$ has a unique element $n_1$ of order 2, and the natural map $Z \times \langle n_1 \rangle \to N$ is an isomorphism (this is the Chinese remainder theorem); here $\langle n_1 \rangle \cong \mathbb{Z}/2\mathbb{Z}$ is the subgroup generated by $n_1$. Since $N_1$ is normal, any $g \in G$ acts on $N_1$ by conjugation. This action fixes each element of $Z$ (since these elements are central) and fixes $n_1$ (since it is the unique order 2 element of $N_1$), and therefore fixes every element of $N_1$. We thus see that $N_1$ is central; similary for $N_2$.

Since $G = N_1N_2$, it follows that $G$ is commutative. The exact sequence

$$1 \to Z \to N_1 \times N_2 \to G \to 1$$

now yields the stated result. (The first map above is $z \mapsto (z, z^{-1})$, and the second map is $(g_1, g_2) \mapsto g_1g_2$.)