**Problem.** Let $p$ be prime and let $\mathbb{F}_p$ be the field with $p$ elements. Let $G$ be the group $\text{GL}_n(\mathbb{F}_p)$ with $n \geq 2$ and let $G$ act on $(\mathbb{F}_p^n)^2$ in the obvious way. How many orbits does $G$ have on $(\mathbb{F}_p^n)^2$? (The “obvious way” is that, for $g \in \text{GL}_n(\mathbb{F}_p)$, and $\vec{x}, \vec{y} \in \mathbb{F}_p^n$, we have $g \ast (\vec{x}, \vec{y}) = (g\vec{x}, g\vec{y})$.)

**Solution.** Let $V = \mathbb{F}_p^n$ with standard basis $e_1, \ldots, e_n$, and let $x, y \in V$. We consider several cases.

1. If $x = y = 0$ then $G$ fixes $(x, y)$, i.e., it makes up a single orbit.
2. Suppose $x = 0$ and $y \neq 0$. Since $G$ acts transitively on $V \setminus \{0\}$, we can move $y$ to $e_1$. Thus this case contributes a single orbit.
3. Suppose $x \neq 0$ and $y$ is linearly dependent on $x$, i.e., $y = cx$ for some $c \in \mathbb{F}_p$. The equation $y = cx$ is preserved by the group $G$, and so $c$ is an invariant of the orbit of $(x, y)$. Using $G$, we can then move $x$ to $e_1$, and $y$ will move to $ce_1$. We thus see that $c$ is the only invariant of the orbit, and so there are $p$ orbits in this case (amounting to the $p$ choices of $c$).
4. Finally, if $x$ and $y$ are linearly independent then we can move $(x, y)$ to $(e_1, e_2)$. Thus there is one orbit in this case.

In total, there are $p + 3$ orbits.

**Problem.** Let $G$ be a group of order 2023. Show that $G$ is abelian. We will helpfully tell you that $2023 = 7 \times 17^2$.

**Solution.** By the third Sylow theorem, the number of 7-Sylows divides $17^2$ (and is thus 1, 17, or $17^2$), and is congruent to 1 modulo 7. Since $17 \equiv 3 \pmod{7}$, we have $17^2 \equiv 2 \pmod{7}$, and so the number of 7-Sylows must be 1. Similarly, the number of 17-Sylows divides 7 and is congruent to 1 modulo 17, and thus must be 1.

Let $H$ and $K$ be the unique 7-Sylow and 17-Sylow. Then $H$ and $K$ are normal, $G = HK$ (look at orders), and $H \cap K = 1$ (look at orders). Thus $G = H \times K$. Since any group of order $p$ or $p^2$ (with $p$ prime) is abelian, we see that $H$ and $K$ are abelian, and so $G$ is as well.

**Problem.** Let $n$ be a positive integer. The dihedral group of order $2n$, written $D_{2n}$, is defined to be the group generated by two elements $\rho$ and $\sigma$, modulo the relations $\sigma^2 = \rho^n = e$ and $\sigma\rho = \rho^{-1}\sigma$. Show that the abelianization of $D_{2n}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if $n$ is odd and is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ if $n$ is even. (The abelianization of a group $G$ is the quotient of $G$ by the subgroup generated by all elements of the form $ghg^{-1}h^{-1}$.)

**Solution.** The abelianization is the quotient of $\mathbb{Z}\sigma \oplus \mathbb{Z}\rho$ by the relations

$$2\sigma = 0, \quad n\rho = 0, \quad \sigma + \rho = -\rho + \sigma.$$ 

Of course, the third relation just amounts to $2\rho = 0$. We thus obtain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/(2,n)\mathbb{Z}$, where $(2,n)$ denotes the ideal of $\mathbb{Z}$ generated by 2 and $n$. We have $(2,n) = (2)$ if $n$ is even and $(2,n) = (1)$ if $n$ is odd, and so the result follows.

**Problem.** Let $L/\mathbb{Q}$ be a Galois extension of degree $2^n$ for some positive integer $n$. Show that there is some nonsquare rational number $D$ such that $\sqrt{D} \in L$.
**Solution.** Let $G$ be the Galois group of $L/\mathbb{Q}$, which has order $2^n$. Since $G$ is a non-trivial 2-group, there is a surjection $G \to \mathbb{Z}/2\mathbb{Z}$. By Galois theory, this means there is an intermediate field $E$ to $L/\mathbb{Q}$ of degree 2 over $\mathbb{Q}$. By the classification of quadratic fields, $E = \mathbb{Q}(\sqrt{D})$ for some nonsquare $D \in \mathbb{Q}$.

**Problem.** Let $L$ be the field $\mathbb{C}(x_1, x_2, \ldots, x_n)$; in other words, the field of rational functions in $n$ algebraically independent variables $x_1, x_2, \ldots, x_n$ with coefficients in $\mathbb{C}$. Let $K$ be the subfield $\mathbb{C}(x_1^2, x_2^2, \ldots, x_n^2)$. Show that $K(x_1 + x_2 + \cdots + x_n) = L$. (In other words, show that $x_1 + x_2 + \cdots + x_n$ is a primitive element for the extension $L/K$.)

**Solution.** Let $\sigma_i$ be the field automorphism of $L$ given by $\sigma_i(x_i) = -x_i$ and $\sigma_i(x_j) = x_j$ for $j \neq i$. The $\sigma_i$’s fix $K$, and generate a subgroup of $\text{Gal}(L/K)$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. Since $L/K$ has degree $2^n$, this must be the full Galois group and $L/K$ is Galois. Let $\sigma$ be an arbitrary element of $G$. Write $\sigma = \sigma_1^{a_1} \cdots \sigma_n^{a_n}$ with $a_i \in \{0, 1\}$. Put $\theta = x_1 + \cdots + x_n$. Then

$$\sigma \theta = (-1)^{a_1} x_1 + \cdots + (-1)^{a_n} x_n.$$  

We thus see that if $\sigma \neq 1$ then $\sigma \theta \neq \theta$. In other words, if $H \subset G$ then $\theta$ belongs to the fixed field $L^H$ if and only if $H$ is trivial. Thus $L = K(\theta)$ by Galois theory.