Problem 1. Let G be a simple group. Let H be a normal subgroup of $G \times G$. Show that H is isomorphic to either the trivial group, to G or to $G \times G$.

Solution Let $K = H \cap (G \times \{1\})$, since H is normal in $G \times G$ we know that K is normal in G, and is thus either $\{e\}$ or G. Let L be the projection of H onto the second factor; the image of a normal subgroup under a surjective homomorphism is normal, so L is normal in G, and thus $L = \{e\}$ or G. So we have a short exact sequence $1 \to K \to H \to L \to 1$ where each of K and L are either $\{e\}$ or G. If $K = L = \{e\}$ then $H \cong \{e\}$; if one of K and L is trivial and the other is G then $H \cong G$, and if $K = L = G$ then $H = G \times G$.

Problem 2. Let p be a prime. Let G be a group such that $|G|$ is divisible by p but not by p^2. Show that G contains at most $p-1$ conjugacy classes of elements of order p.

Solution Let σ be an element of order p in G. We will show that any other element τ of order p is conjugate to one of σ, σ^2, …, σ^{p-1}.

Since p divides $|G|$ and p^2 does not, the cyclic group $\langle \sigma \rangle$ is a p-Sylow subgroup of G, as is $\langle \tau \rangle$. So $\langle \sigma \rangle$ is conjugate to $\langle \tau \rangle$. This means that τ must be conjugate to some generator of $\langle \sigma \rangle$, as claimed above.

Problem 3. Let p be a prime. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ whose order is prime to p. Let $\pi : \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the reduction modulo p map. Show that there is a group homomorphism $\sigma : G \to \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ such that $\pi(\sigma(g)) = g$ for all $g \in G$.

Solution Let $\pi : \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the reduction map modulo p. Let $H = \pi^{-1}(G)$ and let K be the kernel of π. Then we have a short exact sequence $1 \to K \to H \xrightarrow{\pi} G \to 1$. Now, $|K| = p^4$ and $|H|$ is relatively prime to p. So, by the Schur-Zassenhaus theorem, this sequence is semidirect. The right splitting $\sigma : G \to H \subset \mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ is the required map.

Problem 4. Let ζ be a primitive 25th root of 1 over $\mathbb{Q}$. Show that the equation $X^5 - 5$ has no solutions over $\mathbb{Q}[\zeta]$.

Solution We first note that $\mathbb{Q}(\zeta)$ is Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/25\mathbb{Z})^\times$. (Technically, this solution will only need that the Galois group is a subgroup of $(\mathbb{Z}/25\mathbb{Z})^\times$, which is somewhat easier to show.)

Let K be the splitting field of $x^5 - 5$ over $\mathbb{Q}$. By a standard computation, $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$.

Suppose for the sake of contradiction that $x^5 - 5$ has a root α in $\mathbb{Q}(\zeta)$. Then $\alpha\zeta^5$, $\alpha\zeta^{10}$, $\alpha\zeta^{15}$, $\alpha\zeta^{20}$ are also be roots of $x^5 - 5$ in $\mathbb{Q}(\zeta)$, so $x^5 - 5$ splits in $\mathbb{Q}(\zeta)$ and thus K is a subfield of $\mathbb{Q}(\zeta)$. So $\mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$ must be a quotient group of $(\mathbb{Z}/25\mathbb{Z})^\times$ (or, if we only know that the Galois group is a subgroup of $(\mathbb{Z}/25\mathbb{Z})^\times$, must be a quotient of this subgroup). Since $(\mathbb{Z}/25\mathbb{Z})^\times$ (and its subgroups) are abelian, it cannot surject onto the non-abelian group $\mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$, a contradiction.

Problem 5. Let p be a prime, let k be a field in which $p \neq 0$ and let $f(x)$ be the polynomial $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$. Let $g_1(x)g_2(x)\cdots g_r(x)$ be the factorization of $f(x)$ into irreducibles in $k[x]$. Show that all the polynomials $g_i(x)$ have the same degree.

Solution Let ζ, ζ^2, ζ^3, …, ζ^{p-1} be the roots of $f(x)$ in the algebraic closure of k. The Galois group of $k(\zeta)/k$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$, with $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ acting by $\zeta^i \mapsto \zeta^{ai}$; let H be this subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $(x - \zeta^i)$ and $(x - \zeta^j)$ divide the same factor $g_k(x)$

if and only if i and j are in the same $\mathrm{Gal}(k(\zeta)/k)$ orbit or, equivalent, if i and j are in the same coset of H. So each polynomial g_k has degree $|H|$.