Let $P$ be an $n \times n$ matrix with entries in a field and satisfying $P^2 = P$. What are the possible values of $\text{Tr}(P)$?

If $\lambda$ is an eigenvalue of $P$ (in any algebraic closure), then $\lambda^2 = \lambda$, so $\lambda = 0$ or $1$. The trace, being the sum of the eigenvalues counted with multiplicity, must then be an integer between 0 and $n$. If $Q$ is a diagonal matrix with $i$ ones and $(n-i)$ zeroes on the diagonal, then $Q^2 = Q$ and $\text{Tr}(Q) = i$, so all possibilities can occur.

Let $L/K$ be a Galois extension with Galois group $\mathbb{Z}/4\mathbb{Z}$ and characteristic of $K$ not equal to 2. Let $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ be an orbit for the Galois action on $L$, with a generator for the Galois action being $\theta_1 \mapsto \theta_2 \mapsto \theta_3 \mapsto \theta_4 \mapsto \theta_1$. Let $Q$ be the quadratic extension of $K$ contained in $L$. In terms of the $\theta_i$, write down an element $\beta$ of $K$ so that $Q = K(\sqrt{\beta})$.

Let $\sigma$ be a generator of $\text{Gal}(L/K)$ acting on the $\theta_i$ as $\theta_1 \mapsto \theta_2 \mapsto \theta_3 \mapsto \theta_4 \mapsto \theta_1$. If $\beta \in K$ is such that $Q = K(\sqrt{\beta})$, then $\sqrt{\beta}$ must satisfy

$$\sigma^2(\sqrt{\beta}) = \sqrt{\beta}, \quad \text{and} \quad \sigma(\sqrt{\beta}) = -\sqrt{\beta}.$$ 

Thus a candidate for $\sqrt{\beta}$ is

$$\sqrt{\beta} := \theta_1 - \theta_2 + \theta_3 - \theta_4,$$

and so we may take

$$\beta = (\theta_1 - \theta_2 + \theta_3 - \theta_4)^2,$$

as long as this expression is nonzero. If it is zero, then instead one may take $\beta = (\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)^2$. (If both these choices of $\beta$ are zero, then $\theta_1 + \theta_3 = \theta_2 + \theta_4$, and $\theta_1^2 + \theta_3^2 = \theta_2^2 + \theta_4^2$, from which it follows that $\{\theta_1, \theta_3\} = \{\theta_2, \theta_4\}$ as sets, which is not possible since the $\theta_i$ are distinct.)

Alternate solution: Take

$$\beta = \prod_{i<j}(\theta_i - \theta_j)^2.$$ 

This is nonzero and it is easy to see that it has the required property.

Let $G$ be a finite group and $p$ a prime. Recall that a subgroup $P$ of $G$ is called a $p$-Sylow subgroup if $|G| = p^m m$ for $m$ relatively prime to $p$ and $|P| = p^k$. Let $G$ and $H$ be finite groups. Show that every Sylow subgroup of $G \times H$ is of the form $P \times Q$ for $P$ a Sylow subgroup of $G$ and $Q$ a Sylow subgroup of $H$.

Suppose that the exact powers of $p$ dividing $|G|$ and $|H|$ are $p^r$ and $p^s$ respectively. Let $K$ be a $p$-Sylow subgroup of $G \times H$, so $K$ has order $p^{r+s}$. Identify $G$ and $H$ with the subgroups $G \times 1$ and $1 \times H$ of $G \times H$. Let $P = K \cap G$ and $Q = K \cap H$. Let $\varphi$ be the composite map

$$K \rightarrow G \times H \rightarrow G,$$
where the first map is the inclusion of $K$ in $G \times H$ and the second is the projection onto the second factor. Then $\ker(\varphi) = Q$, being a $p$-group contained in $H$, has size bounded by $p^r$. Also, $\text{image}(\varphi)$, being a $p$-group contained in $G$, has size bounded by $p^s$. Since $|K| = p^{r+s}$, it follows that $|Q| = p^s$. Likewise, $|P| = p^r$ and hence $|P \times Q| = p^{r+s}$. Since $P \times Q$ is contained in $K$, it follows that $K = P \times Q$.

Alternate Solution: Let the exact powers of $p$ dividing $|G|$ and $|H|$ are $p^r$ and $p^s$ respectively. Let $P$ be a $p$-Sylow of $G$ and let $Q$ be a $p$-Sylow of $H$. Then $|P \times Q| = p^r \cdot p^s = p^{r+s}$, and is thus a $p$-Sylow of $G \times H$. Any two $p$-Sylows of $G \times H$ are conjugate, so every $p$-Sylow of $G \times H$ is of the form $(g, h)(P \times Q)(g, h)^{-1} = (gP g^{-1}) \times (hQ h^{-1})$. We are done, as $gP g^{-1}$ and $hQ h^{-1}$ are $p$-Sylows of $G$ and $H$ respectively.

(4) Let $A$ be an $n \times n$ matrix over a field $k$. Let $L_A$ be the linear map 

$$M_{n \times n}(k) \to M_{n \times n}(k), \quad X \mapsto A \cdot X.$$ 

Is the characteristic polynomial of $L_A$ determined by the characteristic polynomial of $A$?

Let $k^n$ be the space of column vectors of length $n$ and let $\varphi_A : k^n \to k^n$ be the (left) multiplication by $A$ map. We can identify $M_{n \times n}(k)$ with $k^n \otimes k^n$ via the map sending $e_{ij}$ to $e_i \otimes e_j$. Via this identification, the linear map $L_A$ is just $\varphi_A \otimes 1$, hence the characteristic polynomial of $L_A$ is the $n$th power of the characteristic polynomial of $A$.

(5) $A$ is a finite abelian group in which every element has order dividing 63 and in which there are 108 elements of order exactly 63. Determine all possibilities for the structure of $A$.

By the structure theorem for finite abelian groups, $A$ must be a sum of some number of copies of $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$, with at least one copy each of $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$. Suppose that $$A \cong (\mathbb{Z}/3\mathbb{Z})^a \oplus (\mathbb{Z}/9\mathbb{Z})^b \oplus (\mathbb{Z}/7\mathbb{Z})^c,$$

with $b, c \geq 1$. The number of elements in $A$ of order exactly 63 is then

$$3^a \cdot (9^b - 3^b) \cdot (7^c - 1).$$

Since $7^c - 1$ must divide 108, it follows that $c = 1$. Then $a = b = c = 1$ is the only solution. Thus,

$$A \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}.$$
(1) Let \( G \) be a finite group, and let \( A \) and \( B \) be subgroups of \( G \) with \( |G| = |A||B| \) and \( \gcd(|A|, |B|) = 1 \). Show that every element of \( G \) can be uniquely written as \( ab \) with \( a \in A \) and \( b \in B \).

First observe that \( A \cap B = 1 \) since \( \gcd(|A|, |B|) = 1 \). Let \( f : A \times B \to G \) be the map (of sets) given by

\[
f(a, b) = a \cdot b.
\]

We claim that \( f \) is injective. Indeed,

\[
f(a, b) = f(a', b') \Rightarrow a \cdot b = a' \cdot b' \Rightarrow (a')^{-1} \cdot a = b' \cdot b^{-1} \in A \cap B = 1,
\]

so \( a' = a \) and \( b' = b \). Since \( f \) is injective, and \( |G| = |A||B| = |A \times B| \), it follows that \( f \) must be surjective as well. Thus \( f \) is bijective, which is the same thing as saying that every element of \( G \) can be written uniquely as \( ab \) with \( a \in A \) and \( b \in B \).

(2) Let \( L/F \) be a Galois extension with Galois group \( \text{GL}_2(\mathbb{F}_p) \). Let \( H \) be the subgroup \( \left( \begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix} \right) \) of \( G \) and let \( K \) be its fixed field.

(a) What is the group \( \{ g \in \text{GL}_2(\mathbb{F}_p) : gK = K \} \)?

(b) What is the group of automorphisms of \( K \) that fix \( F \)? Please identify these groups as explicitly as possible.

(a) Let us write \( G \) for \( \text{Gal}(L/F) = \text{GL}_2(\mathbb{F}_p) \). By the main theorem of Galois theory,

\[
\{ g \in G : gK = K \} = \{ g \in G : \text{Gal}(L/gK) = \text{Gal}(L/K) \}
= \{ g \in G : g\text{Gal}(L/K)g^{-1} = \text{Gal}(L/K) \}
= N_G(H).
\]

An explicit computation shows that

\[
N_G(H) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}.
\]

(b) Write \( \text{Aut}(K/F) \) for the group of automorphisms of \( K/F \). Note that \( K/F \) is not Galois since \( H \) is not normal in \( G \). However, if \( \sigma \in \text{Aut}(K/F) \), then \( \sigma \) can be extended to an element \( g \) of \( \text{Gal}(L/F) \). By part (a), such a \( g \) must belong to \( N_G(H) \). Conversely, any \( g \in N_G(H) \) when restricted to \( K \), gives an element of \( \text{Aut}(K/F) \). Thus there is a surjective homomorphism

\[
N_G(H) \to \text{Aut}(K/F),
\]

whose kernel is exactly \( H \). Consequently,

\[
\text{Aut}(K/F) \cong N_G(H)/H \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{F}_p^\times \right\} \cong \mathbb{F}_p^\times \times \mathbb{F}_p^\times.
\]

(3) Let \( H \) be the vector space of \( 2 \times 2 \) Hermitian matrices. (A matrix is Hermitian if it is the complex conjugate of its transpose.) Define the quadratic form \( q \) on \( H \) by \( q(M) = \det M \). What is the signature of \( q \)?
A general $2 \times 2$ Hermitian matrix looks like $\begin{pmatrix} w & x+iy \\ -x-iy & z \end{pmatrix}$, with $(w, x, y, z)$ real. Its determinant is $ wz - x^2 - y^2$. Rewriting this as $(\frac{w+z}{2})^2 - (\frac{w-z}{2})^2 - x^2 - y^2$, we see that the signature is $++-$. 

(4) **Classify (up to isomorphism) all groups of order 2013, and prove that your list is complete.** (Note: $2013 = 3 \times 11 \times 61$.)

There are two such groups: $\mathbb{Z}/3 \times \mathbb{Z}/11 \times \mathbb{Z}/61$ and $\mathbb{Z}/11 \times (\mathbb{Z}/3 \rtimes \mathbb{Z}/61)$, where $\mathbb{Z}/3$ acts on $\mathbb{Z}/61$ by multiplication by 13. (Note that $13^3 = 2197 \equiv 1 \mod 61$. Answers which simply stated that there is a nontrivial cube root of 1 modulo 61 without computing it received full credit.)

Let $G$ be a group of order 2013. The number of 61-Sylow’s must be $\equiv 1 \mod 61$. The only divisor of 2013 which is 1 mod 61 is 1, so the 61-Sylow is normal. Also, as 61 is prime, the only group of order 61 is cyclic. So we have a short exact sequence

$$0 \to \mathbb{Z}/61 \to G \to H \to 0$$

where $H$ has order 33. As $33 = 3 \times 11$ and $11 \equiv 1 \mod 3$, the only group of order 33 is $\mathbb{Z}/33$ (also known as $\mathbb{Z}/3 \times \mathbb{Z}/11$). Since 33 and 61 are relatively prime, this short exact sequence must be semidirect.

It remains to find all ways for $\mathbb{Z}/33$ to act on $\mathbb{Z}/61$. The automorphism group of $\mathbb{Z}/61$ is the same as the group of units in the ring $\mathbb{Z}/61$, which is a cyclic group of order 60. So we need to find homomorphisms from $\mathbb{Z}/33$ to $\mathbb{Z}/60$. Since $\text{GCD}(33, 60) = 3$, such a map must send a generator of $\mathbb{Z}/33$ to a 3-torsion element in $\mathbb{Z}/60$.

One possibility is that this 3-torsion element is the identity, meaning that $\mathbb{Z}/33$ acts trivially on $\mathbb{Z}/61$. In this case, the short exact sequence splits and $G \cong \mathbb{Z}/61 \times \mathbb{Z}/33 \cong \mathbb{Z}/61 \times \mathbb{Z}/3 \times \mathbb{Z}/11$.

The other possibility is that this 3-torsion element is one of the two nontrivial cube roots of unity. In this case, $\mathbb{Z}/11$ still acts trivially, so the group breaks up as $\mathbb{Z}/11 \times (\mathbb{Z}/3 \rtimes \mathbb{Z}/61)$. Choosing different cube roots of unity gives isomorphic groups, related by the automorphism $x \mapsto x^{-1}$ of $\mathbb{Z}/3$.

**Bonus: Finding a cube root of 1 modulo 61 by hand.** In any field of characteristic $\neq 2, 3$, the following are equivalent:

- $\zeta^3 = 1$ and $\zeta \neq 1$
- $\zeta^2 + \zeta + 1 = 0$
- $(2\zeta + 1)^2 = -3$

So, we aim to find a square root of $-3$ modulo 61. Looking at square near multiples of 61, we see that $8^2 \equiv 3 \mod 61$ and $11^2 \equiv -1 \mod 61$, so $88^2 \equiv -3 \mod 61$. For ease of computation, we work with 27 rather than 88, as $27 \equiv 88 \mod 61$. So we may take $\zeta = (-1 \pm 27)/2 \mod 61$; this gives us $\zeta = 13$ and $\zeta = 47$ as the nontrivial cube roots of 1.

(5) **Let $R$ be the ring $\mathbb{Z}[X,Y]/(7, X^2 + 3Y^2)$.

(a) Is $R$ a domain? Why or why not?

(b) Classify the prime ideals in $R$ that are not maximal.

Write $F_7$ for the field $\mathbb{Z}/7\mathbb{Z}$. 
The ring $R$ is not a domain. Notice that $(X+2Y)(X-2Y) = X^2 - 4Y^2 = X^2 + 3Y^2 = 0$ in $R$. However, the degree one part of $R$ is $\mathbb{F}_7 X \oplus \mathbb{F}_7 Y$, so $X + 2Y$ and $X - 2Y$ are nonzero.

There are two non-maximal prime ideals: $(X+2Y)$ and $(X-2Y)$. We first show that $(X-2Y)$ is prime and nonmaximal; the proof for $(X+2Y)$ is practically identical. We compute

$$R/(X-2Y) \cong \mathbb{Z}[X,Y]/(7, X - 2Y, X^2 + 3Y^2)$$
$$\cong \mathbb{F}_7[X,Y]/(X-2Y, X^2 - 4Y^2)$$
$$\cong \mathbb{F}_7[X,Y]/(X-2Y)$$
$$\cong \mathbb{F}_7[Y]$$

Note that $\mathbb{F}_7[Y]$ is a domain but not a field, so the ideal is prime but not maximal. (The second isomorphism is because $-4 \equiv 3 \mod 7$, the third is because $X - 2Y$ divides $X^2 - 4Y^2$.)

We now must show that there are no other such ideals. Let $p$ be a prime ideal of $R$. Since $(X-2Y)(X+2Y)$ is 0 in $R$, either $X - 2Y$ or $X + 2Y$ (or both) must be in $p$. Without loss of generality, say that $X - 2Y$ is in $p$. So $R/p$ is a quotient of $R/(X-2Y)$, which we computed above to be isomorphic to $\mathbb{F}_7[Y]$. We are looking for domains which occur as $\mathbb{F}_7[Y]/q$ for an ideal $q$ of $\mathbb{F}_7[Y]$. Such domains are either $\mathbb{F}_7[Y]$ itself, or are $\mathbb{F}_7[Y]/f(Y)$ for an irreducible polynomial $f$. In the latter case, the quotient is the finite field with $7^\deg f$ elements, so the corresponding ideal is maximal. The only case which gives us non-maximal prime ideals is when the quotient is $\mathbb{F}_7[Y]$, which corresponds to the stated ideals.

Alternate solution:

Observe that $R \cong \mathbb{F}_7[X,Y]/(X^2 - 4Y^2) = \mathbb{F}_7[X,Y]/((X + 2Y)(X - 2Y)) \cong \mathbb{F}_7[t,s]/(ts)$, via the change of variables $X + 2Y = t$, $X - 2Y = s$. It is clear from this description that $R$ is not a domain, since $ts = 0$ but neither $t$ nor $s$ is zero in $R$. Prime ideals of $R$ that are not maximal correspond bijectively to primes $p$ in $\mathbb{F}_7[t,s]$ containing $ts$, that are not maximal. Any such prime must contain $t$ or $s$. Suppose that $p \supset (t)$. Since $\mathbb{F}_7[t,s]/(t) \cong \mathbb{F}_7[s]$, and all nonzero prime ideals in $\mathbb{F}_7[s]$ are maximal, it follows that $p = (t)$. Similarly, if $p \supset (s)$, then in fact $p$ must equal $(s)$. In the original coordinates $X, Y$, we find then that the only prime ideals of $R$ that are not maximal are $(X + 2Y)$ and $(X - 2Y)$.