1. Let $V$ be a vector space of dimension $d$ over a field $k$. Let $n$ be an odd number. Let \( \phi : V \otimes n \to V \otimes n \) be the linear map which is given on pure tensors by
\[
\phi(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = v_2 \otimes v_3 \otimes \cdots \otimes v_n \otimes v_1.
\]
Compute (in terms of $d$ and $n$) the trace and determinant of $\phi$.

Let $e_1, e_2, \ldots, e_d$ be a basis for $V$. For $I$ a sequence \((i_1, i_2, \ldots, i_n)\) of indices between 1 and $d$, let $e_I = e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_n}$. Then $\phi$ acts by a permutation matrix on the basis $e_I$.

$\text{Tr}(\phi)$ is the number of $e_I$ which are fixed by $\phi$. The vector $e_I$ is fixed by $\phi$ if and only if $i_1 = i_2 = \cdots = i_n$, so there are $d$ such vector and $\text{Tr}(\phi) = d$.

Since $\phi$ is a permutation matrix of odd order (using that $n$ is odd) we deduce that $\text{det} \phi = 1$.

2. Let $G$ be a simple group of order 360. How many 5-Sylow subgroups does $G$ have? (If your proof involves classifying the simple group(s) of order 360, then you must prove your classification to be correct.)

The number of 5-Sylow subgroups divides 72 and is congruent to 1 mod 5, hence is either 1, 6 or 36. We show that there are 36 such subgroups. The number of 5-Sylows cannot be 1 since then the unique 5-Sylow would be normal in $G$, contradicting the simplicity of $G$. So let us assume that $G$ has exactly 6 5-Sylow subgroups and derive a contradiction.

Let $\Sigma$ be the set of 5-Sylow subgroups of $G$ and consider the action of $G$ on $\Sigma$ by conjugation. This gives a homomorphism $\varphi : G \to S_6$, which is nontrivial since $G$ acts transitively on $\Sigma$. Since $G$ is simple, $\varphi$ is an injection, so we may identify $G$ with a subgroup of $S_6$. Now $|G| = 360 = |A_6|$, hence $|G \cap A_6| > 1$. But $G \cap A_6$ is normal both in $G$ and $A_6$. By the simplicity of $G$ (or of $A_6$), it follows that $G = A_6$. However $A_6$ has (strictly) more than 6 5-Sylow subgroups. Contradiction.

Remark: In fact, there is only one simple group of order 360 (up to isomorphism). It can be variously described as $A_6$ or as $PSL(2, F_9)$.

3. Let $k$ be a field of characteristic zero containing a nontrivial cube root of unity. Let $\alpha$ and $\beta$ be nonzero elements of $k$. Show that, if $[k(\sqrt[3]{\alpha}, \sqrt[3]{\beta}) : k] < 9$, then at least one of $\alpha$, $\beta$, $\alpha \beta$ or $\alpha/\beta$ is a cube in $k$.

Let $E$, $F$, $L$ denote the fields $k(\sqrt[3]{\alpha})$, $k(\sqrt[3]{\beta})$ and $k(\sqrt[3]{\alpha}, \sqrt[3]{\beta})$ respectively. Note that this notation makes sense since $k$ contains a primitive cube root of unity $\omega$, hence the field obtained by adjoining any third root of $\alpha$ contains all the third roots of $\alpha$ and is Galois over $k$. We may suppose that $\alpha$ and $\beta$ are not cubes in $k$. Then $[E : k] = [F : k] = 3$. Since $L = E[\sqrt[3]{\beta}]$, and $E$ contains $\omega$, it follows that $[L : E] = 3$ or 1. If $[L : E] = 3$, then $[L : k] = 9$ contradicting the fact that $[L : k] < 9$. Thus $[L : E] = 1$ and $E = L = F$. Now write $\text{Gal}(L/k) = \{1, \sigma, \sigma^2\}$ and consider the action of $\sigma$ on $\sqrt[3]{\alpha}$ and $\sqrt[3]{\beta}$. We have:
\[
\sigma(\sqrt[3]{\alpha}) = \omega^{\pm 1} \cdot \sqrt[3]{\alpha}
\]
and
\[
\sigma(\sqrt[3]{\beta}) = \omega^{\pm 1} \cdot \sqrt[3]{\beta}.
\]
Thus $\sigma$ fixes either $\sqrt[3]{\alpha} \cdot \sqrt[3]{\beta}$ or $\sqrt[3]{\alpha}/\sqrt[3]{\beta}$ and hence at least one of these elements lives in $k$, as was to be shown.
4. Let $A$ be an $n \times n$ matrix with entries in a field $k$. Let $\psi : \text{Mat}_{n \times n}(k) \to \text{Mat}_{n \times n}(k)$ be the map $X \mapsto AX -XA$. Show that the kernel of $\psi$ has dimension $\geq n$.

We may extend scalars and assume that $k$ is algebraically closed. Further, conjugating by an invertible matrix $P$ we may assume that $A$ is in Jordan form. If $A = A_1 \oplus \cdots \oplus A_r$ is a sum of Jordan blocks and if the result is true for each $A_i$, then it is true for $A$. This follows from the observation that if $\varphi_i$ is the map attached to $A_i$ and $X_i$ is in the kernel of $\varphi_i$, then $X_1 \oplus X_2 \cdots \oplus X_r$ is in the kernel of $\varphi$.

Thus we are reduced to the case of $A$ being a single Jordan block, namely the minimal polynomial of $A$ equals its characteristic polynomial. Then the span of the powers $A^t$ has dimension $n$ and is in the kernel of $\psi$, so we are done.

5. Let $G$ be a finite group with $c > 1$ conjugacy classes. Show that $G$ contains a nonidentity element of order $\leq c$.

Write the class equation of $G$:

$$|G| = \sum |a| |G| / |C_a|,$$

where the sum is over conjugacy classes $[a]$ and $C_a$ is the centralizer of the element $a$. In the sum on the right there are exactly $c$ terms, hence at least one term is of size $\geq |G| / c$. For this term $[a]$, we have

$$\frac{|G|}{|C_a|} \geq \frac{|G|}{c}, \; \text{hence} \; |C_a| \leq c.$$

Since $c > 1$, the group $G$ is not the trivial group with one element, hence $|C_a| > 1$. Let $p$ be a prime dividing $|C_a|$, so that $p \leq c$. By Cauchy’s theorem, $C_a$ (and hence $G$) contains an element of order $p$. 


Afternoon Exam

1. Let $V$ be a vector space of dimension 7 over a field $k$ and let $v$ be an element of $V$. Let $L_v$ be the linear map $x \mapsto x \wedge v$ from $\bigwedge^i V$ to $\bigwedge^{i+1} V$.

Prove or disprove: For every $y \in \bigwedge^3 V$, there is a vector $v$ in $V$ so that $y$ is in the image of $L_v$.

This is false. Suppose $\{e_1, \ldots, e_7\}$ is a basis for $V$. Consider the vector

$$y = e_1 \wedge e_2 \wedge e_3 + e_4 \wedge e_5 \wedge e_6.$$ 

We claim that $y$ is not in the image of $L_v$ for any $v$. Indeed for any $v$ in $V$ and $x \in \bigwedge^2 V$, we have

$$L_v(x) \wedge v = x \wedge v \wedge v = 0.$$ 

However we can check that if $v$ is any nonzero element of $V$, then

$$y \wedge v \neq 0.$$ 

To see this, suppose that $v = \sum_i a_i v_i$. Then

$$y \wedge v = -\sum_{i=1}^3 a_i e_i \wedge e_4 \wedge e_5 \wedge e_6 + \sum_{j=4}^6 a_j e_3 \wedge e_j.$$ 

It follows from this expression that $y \wedge v$ can only be zero if all the $a_i$ are 0, that is if $v = 0$.

2. Let $S_n$ denote the symmetric group on $n$ elements, for $n \geq 1$. Show that there is no injective homomorphism from $S_{n+1}$ into $S_n \times S_n$.

Suppose first that $n \geq 4$ so that $A_{n+1}$ is simple, and suppose that there exists an injection $S_{n+1} \to S_n \times S_n$. Let $H$ and $K$ denote the kernels of the two homomorphisms $S_{n+1} \to S_n$ obtained by projecting onto the first and second factors respectively. Then $H$ is a normal subgroup of $S_{n+1}$ of order at least $n+1$, hence $H \supseteq A_{n+1}$. Likewise, $K \supseteq A_{n+1}$. But the kernel of $S_{n+1} \to S_n \times S_n$ is exactly $H \cap K$, contradiction. For $n = 1, 2, 3$ it is easy to see that such an injection does not exists since in all these cases, $|S_{n+1}|$ does not divide $|S_n|^2$.

3. Let $k$ be a perfect field of characteristic $p$ and let $a$ and $b$ be elements of $k$ with $b \neq 0$. Let $L$ be the splitting field of the polynomial $x^{p^2} + ax^p + bx$.

Show that $\text{Gal}(L/k)$ is a subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $f(x) = x^{p^2} + ax^p + bx$ and $S$ the set of roots of $f$ in $L$. Since $f'(x) = b \neq 0$, the polynomials $f$ and $f'$ have no common roots. Thus $S$ has cardinality exactly $p^2$.

Note that if $\alpha$ and $\beta$ are roots of $f$, then so is $\alpha \pm \beta$. Hence $S$ is a subgroup of the additive group of $k$. Since $k$ has characteristic $p$, this makes $S$ a vector space over $\mathbb{Z}/p\mathbb{Z}$. Pick a basis $\{\alpha, \beta\}$ of $S$ over $\mathbb{Z}/p\mathbb{Z}$. Define the map

$$\rho : \text{Gal}(L/k) \to \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

by

$$\begin{pmatrix} \sigma \alpha \\ \sigma \beta \end{pmatrix} = \rho(\sigma) \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \sigma \in \text{Gal}(L/k).$$

Then $\rho$ is a homomorphism, and is injective since the action of $\sigma$ is determined completely by its action on $\alpha$ and $\beta$. This exhibits $\text{Gal}(L/k)$ as a subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

4. Let $f(x) \in \mathbb{R}[x]$ be a degree $n$ polynomial with distinct roots, $r$ of which are real and $2s$ of which are complex. Let $A$ be the ring $\mathbb{R}[x]/f(x)$.
Let $m_g$ be the map $h \mapsto gh$ from $A$ to $A$. Let $\text{Tr}(g)$ be the trace of $m_g$ considered as an $\mathbb{R}$-linear endomorphism of the real vector space $A$.

Compute the signature of the quadratic form on $A$ given by $\langle g, h \rangle = \text{Tr}(gh)$.

Note that by the Chinese remainder theorem, we have $R \simeq \mathbb{R}^r \oplus \mathbb{C}^s$ and the quadratic form is diagonal with respect to this decomposition. So we just need to compute the signature of the form $\langle g, h \rangle = \text{tr}(gh)$ on $\mathbb{R}$ and $\mathbb{C}$. On $\mathbb{R}$, this is 1, while on $\mathbb{C}$, it is 1, $-1$ as one sees by computing using the basis $\{1, i\}$ for instance. Thus the signature of the original form is $1, 1, \cdots, 1, -1, -1, \cdots -1$ with 1 occurring $r + s$ times and $-1$ occurring $s$ times.

5. Let $R$ be a ring (containing 1, not necessarily commutative). Let $R^\times$ be the unit group of $R$. Show that, if $|R^\times|$ is odd and 5 divides $|R^\times|$, then 15 divides $|R^\times|$.

Let $s$ be an element in $R^\times$ of order 5 and let $S$ be the subring of $R$ generated by 1 and $s$. Then $S$ is a commutative ring. Since $S^\times$ is a subgroup of $R^\times$, we see that $|S^\times|$ is odd as well, so $1 = -1$ in $S$. (Otherwise, $\{1, -1\}$ would be a subgroup of $|S^\times|$ of order 2.) Thus $S \supset \mathbb{Z}/2 = \mathbb{F}_2$, and in fact equals $\mathbb{F}_2[s]$, so is a finite ring. Let 

$$\varphi : \mathbb{F}_2[X] \rightarrow S$$

be the map sending $X$ to $s$. Then $\ker(\varphi)$ is an ideal in $\mathbb{F}_2[X]$, necessarily of the form $f(X)$ for some monic polynomial $f(X)$ in $\mathbb{F}_2[X]$ dividing $X^5 - 1$, and 

$$S \simeq \mathbb{F}_2[X]/f(X).$$

The polynomial $X^5 - 1$ decomposes as 

$$X^5 - 1 = (X - 1)g(X), \quad g(X) = X^4 + X^3 + X^2 + X + 1,$$

where $X - 1$ and $g(X)$ are both irreducible over $\mathbb{F}_2$. Now $f(X)$ cannot be 1, or $S$ would be the zero ring, nor can it be $X - 1$ since then $S \simeq \mathbb{F}_2$ would not contain an element of order 5. It follows that either 

$$S \simeq \mathbb{F}_2[X]/(g(X)) \quad \text{or} \quad S \simeq \mathbb{F}_2[X]/(X^5 - 1) = \mathbb{F}_2 \times \mathbb{F}_2[X]/g(X).$$

Since $\mathbb{F}_2[X]/g(X)$ is a finite field with 16 elements, the order of its unit group is 15. In any case, $|S^\times| = 15$, hence $|R^\times|$ is divisible by 15.