1. Let \( n \geq 5 \).
   (a) Show that the only proper normal subgroup of \( S_n \) is \( A_n \).
   (b) Let \( H \) be a proper subgroup of \( S_n \). Show that either \( H = A_n \) or \( |S_n : H| \geq n \). [Hint: Consider the action of \( S_n \) on \( S_n/H \).]

   \textbf{Proof.} (a): If \( H \triangleleft S_n \) then \( H \triangleleft A_n \) so is either 1 or \( A_n \). If \( H = A_n \) and \( H \) is proper then \( H = A_n \).
   If \( H \cap A_n = 1 \) then \( H \) contains some odd permutation \( \sigma \in H \cap S_n - A_n \). Thus \( S_n = H A_n \) and by the second isomorphism theorem \( |S_n| = |HA_n| = |H| A_n|/|H \cap A_n| = |H| A_n| \) and so \( |H| = 2 \) which means that \( H = \langle (ij) \rangle \) for some transposition. But this is not normal.

   (b): As in class get a homomorphism \( f : S_n \rightarrow S_{S_n/H} \) with kernel contained in \( H \). This kernel is normal in \( S_n \) so is either \( A_n \) or 1. If \( A_n \) then \( H \) contains \( A_n \) and so \( H = A_n \). Otherwise \( S \) injects into \( S_{S_n/H} \) and so \( n! = |S_n| \leq |S_n : H| = |S_{S_n/H}| / |S_n : H| \geq n \).

2. Let \( G \) be a finite group and \( N \) the intersection of all \( p \)-Sylow subgroups of \( G \). Show that \( N \) is a normal \( p \)-subgroup of \( G \) and that every normal \( p \)-subgroup of \( G \) is contained in \( N \).

   \textbf{Proof.} Let \( P \in \text{Syl}_p(G) \) in which case \( N = \cap gP^{-1} \). Thus \( xN x^{-1} = \cap xgP(xg)^{-1} = \cap gPg^{-1} = N \) so \( N \) is normal. Suppose \( H \) is a normal \( p \) group. Then \( H \subset P \) for some \( p \)-Sylow \( P \). But then \( gHg^{-1} = H \subset gPg^{-1} \) for all \( g \) so \( H \subset \cap gPg^{-1} = N \).

3. Let \( 2 < p < q \) be two primes such that \( p \mid q + 1 \). Let \( G \) be a group with \( |G| = p^2q^2 \).
   (a) Show that there is a normal \( q \)-Sylow subgroup \( Q \) of \( G \). [Hint: Show that \( q \mid p^2 - 1 \).]
   (b) Let \( P \) be a \( p \)-Sylow subgroup. Show that \( G \cong Q \rtimes P \).
   (c) If \( Q \) is cyclic show that \( G \) is abelian.
   (d) List all isomorphism classes of abelian groups of order \( p^2q^2 \) with \( p \neq q \).

   There are nonabelian \( G \) of the form \((\mathbb{Z}/q\mathbb{Z})^2 \times (\mathbb{Z}/p\mathbb{Z})^2\), at least two nonisomorphic such semidirect products. Cf. \url{http://www.icm.tu-bs.de/ag_algebra/software/small/number.html}

   \textbf{Proof.} (a): \( n_q \equiv 1 \pmod{q} \) and \( n_q \mid p^2 \). Since \( p < q \) we have \( n_q \neq p \). If \( n_q = p^2 \) then \( q \mid p^2 - 1 \) so either \( q \mid p - 1 \) or \( q \mid p + 1 \). The first case is not possible as \( q > p \) and the second case is only possible if \( q = p + 1 \) but that cannot be as \( p > 2 \) and both \( p \) and \( q \) are prime. Thus \( n_q = 1 \) as desired.

   (b): \( P \cap Q = 1 \) as the two orders are coprime. Also \( PQ \) is a subgroup as \( Q \) is normal and has order \(|PQ| = |P||Q|/|P \cap Q| = p^2q^2 = |G| \) so \( G = PQ \) which implies that \( G \cong Q \rtimes P \).

   (c): If \( Q \) is cyclic then \( G \cong Q \rtimes f \) for some homomorphism \( f : P \rightarrow \text{Aut}(Q) \cong \text{Aut}(\mathbb{Z}/q^2\mathbb{Z}) \cong (\mathbb{Z}/q^2\mathbb{Z})^\times \cong \mathbb{Z}/q(q-1)\mathbb{Z} \). But \(|\text{Im } f| \leq |P| = p^2 \) and \(|\text{Aut}(Q)| = q(q-1) \) and so \(|\text{Im } f| = q(q-1) \) and so \(|\text{Im } f| = 1 \).
(p^2, q(q - 1)) = 1 as p ∤ q - 1 since p ∤ q + 1 but p ≠ 2. Thus f is trivial and G = P × Q. Since P and Q have prime square order they are abelian so G is abelian.

(d): Write p^2q^2 = \prod n_i with \( n_r \mid n_{r-1} \mid \ldots \mid n_1 \) so only 4 possibilities \( p^2q^2 = p^2q^2 = p^2q \cdot q = pq^2 \cdot p = pq \cdot pq \) giving \( \mathbb{Z}/(pq)^2, \mathbb{Z}/pq \times \mathbb{Z}/q, \mathbb{Z}/pq^2 \times \mathbb{Z}/p \) and \( (\mathbb{Z}/pq)^2 \).

4. Let G be a finite group of order 231.

(a) Show that G has normal 7-Sylow and 11-Sylow subgroups.

(b) Show that for groups A, B, C, \((A \rtimes_f B) \times C \cong (A \times C) \rtimes_{f \times \text{id}} B\) where \( f \times \text{id} : B \to \text{Aut}(A) \times \text{Aut}(C) \) sends everything to the trivial automorphism of C.

(c) Show that the unique 11-Sylow subgroup of G is contained in Z(G). [Hint: Use part (b) to express the 11-Sylow subgroup as a direct factor of G.]

Proof. (a): \( n_7 \mid 33 \) and is \( -1 \) (mod 7) so \( n_7 = 1; n_{11} \mid 21 \) and is \( -1 \) mod 11 so \( n_{11} = 1 \).

(b): Consider \( \phi : (A \rtimes_f B) \times C \to (A \times C) \rtimes_{f \times \text{id}} B \) given by \( \phi(a, b, c) = (a, c, b) \). Note that

\[
\phi((a, b, c) \cdot_f (a', b', c')) = \phi(a f_b(a'), bb', cc') = (a f_b(a'), cc', bb') = ((a, c)(f \times \text{id})_b(a', c'), bb') = (a, c, b) \cdot_f \text{id}(a', c', b') = \phi(a, b, c) \cdot_f \text{id} \phi(a', b', c')
\]

so \( \phi \) is a homomorphism which is visibly an isomorphism.

(c): Let P, Q, R be Sylow 3, 7 and 11 subgroups. Here Q and R are normal so \( QR \cong Q \times R \cong \mathbb{Z}/7\mathbb{Z} \) is also normal in G and intersects trivially with P (coprime orders) so \( PQR = G \) (comparing orders) and thus \( G \cong (Q \times R) \times P \). Here the semidirect product is for a homomorphism \( \phi : P \to \text{Aut}(Q \times R) \cong \text{Aut}(Q) \times \text{Aut}(R) \) (since Q and R have coprime orders). Thus \( \phi(x) = (f(x), g(x)) \) where \( f(x) \in \text{Aut}(Q) \) and \( g(x) \in \text{Aut}(R) \). But \( \text{ord}(g(x)) \mid (|P|, |\text{Aut}(R)|) = (3, 10) = 1 \) so \( g(x) = 1 \) for all \( x \) so \( \phi = f \times \text{id} \).

By part (b) we deduce that \( G \cong (Q \times R) \times P \cong (Q \times P) \times R \cong (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}/11\mathbb{Z} \).

Finally, R is abelian and commutes with everything in the direct product \( G \cong (Q \times P) \times R \) so \( R \subset Z(G) \).

5. Let \( \mathbb{F}_q \) be a finite field with \( q \) elements and V an \( n \)-dimensional vector space over \( \mathbb{F}_q \).

(a) Show that \( \text{GL}(n, \mathbb{F}_q) \), the group of \( n \times n \) matrices with coefficients in \( \mathbb{F}_q \) and nonzero determinant, acts \text{simply transitively} on the set of all possible bases of V. Here transitive means that there is one single orbit (for any \( x, y \) there exists \( g \) such that \( gx = y \)) and simple means that if \( gx = x \) for some \( x \) then \( g = 1 \).

(b) Deduce that

\[
| \text{GL}(n, \mathbb{F}_q) | = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})
\]

This formula is useful in random algorithms where it computes the probability that a random matrix is invertible.

Proof. (a): Fix a basis \( e_1, \ldots, e_n \) for \( \mathbb{F}_q^n \). Then \( \text{GL}(n, \mathbb{F}_q) \cong \text{Aut}_{\mathbb{F}_q^\text{vs}}(\mathbb{F}_q^n) \) and a vector space homomorphism is an isomorphism if and only if the span of \( \phi(e_1), \ldots, \phi(e_n) \) is also a basis. Thus the image of \( (e_i) \) under any invertible matrix is a basis and every basis \( v_i = \sum a_{ij}e_j \) is the image of \( (e_i) \) under the necessarily invertible matrix \( (e_{ij}) \). Since matrix multiplication is associative this implies that \( \text{GL}(n) \) acts simply transitively on the set of bases.
(b): The action being simply transitive it follows that the size of the unique orbit (the number of bases) equals the index of the trivial stabilizer inside the group, thus $|\text{GL}(n, \mathbb{F}_q)|$. Thus we only need to count the number of bases. For $v_1$ we can choose any of the nonzero vectors in $\mathbb{F}^n_q$. For $v_2$ we choose any vector in $\mathbb{F}^n_q$ not in the span of $v_1$, etc. Thus the number of bases is $q^n - 1$ choices for $v_1$, $q^n - q$ choices for $v_2$, etc so we get the desired formula. $\Box$