Background:

I: There are three basic methods for coming up with normal subgroups of finite groups.

(1) You can apply the Sylow theorems. For example, the Sylow theorems tell us immediately that a group of order 111 must have a normal subgroup of order 37.

(2) Normal subgroups also arise as isotropy subgroups of group actions. For example, if a Sylow 11-subgroup of a group G of order $1452 = 11^2 * 12$ is not normal, Sylow tells us that there are 12 Sylow 11-subgroups, and that G acts on them transitively by conjugation. This action induces a non-trivial homomorphism $G \to S_{12}$, and since 1452 does not divide 12!, the kernel of the homomorphism (i.e., the isotropy subgroup of the action) is neither G nor (1_G), so G has a non-trivial normal subgroup.

(3) Finally, there are counting arguments. For these it is useful to keep in mind that the union U_p of the conjugates of the Sylow p-subgroups is disjoint (apart from the identity) from the union U_q of the conjugates of the Sylow q-subgroups if $p \neq q$, since $a \in U_p$ has order a positive power of p while $b \in U_q$ has order a positive power of q. Note also that the distinct subgroups of prime order are disjoint, apart from the identity, since any non-identity element of a subgroup of prime order generates the subgroup. We can apply these ideas to show that a group G of order $132 = 11 * 12$ cannot be simple. Let n_p be the number of Sylow p-subgroups in G. If G were simple, Sylow tells us that $n_{11} = 12$, that $n_3 \geq 4$, and that $n_2 \geq 3$. Thus there must be $12(11-1) = 120$ non-identity elements in the union of the Sylow 11-subgroups, and at least $4(3-1) = 8$ non-identity elements in the union of the Sylow 3-subgroups. There are also clearly at least $4+1$ elements in the union of the Sylow 2-subgroups. Since all of these elements must be different, G must have at least $120 + 8 + 5 = 133$ elements. This is impossible since $|G| = 132$.

All three of these techniques come up in Problem [1] (at least, if you do it the way I did it!).

II: The following background will be useful for proving Wedderburn's little theorem (Problem [5] below, that a finite division ring is a field). A *left module* M over a ring R (also known as a left R-module) is an abelian group with an operation $\theta : R \times M \to M$ where we denote $\theta((r,m)$ by rm and we think of the operation as a scalar multiplication, which we require to satisfy the following: $a(bm) = (ab)m$ for all $a, b \in R$ and all $m \in M$; $(a+b)m = am + bm$ for all $a, b \in R$ and all $m \in M$; and $a(m+n) = am + an$ for all $a \in R$ and $m, n \in M$. Lang also requires $1_R m = m$ for all $m \in M$, while Hungerford calls a module satisfying this condition a *unitary* R-module. We'll go by Lang's definition. When R is not commutative, one can also define a right R-module where the multiplication is on the right. When R is commutative, every left R-module automatically has a right R-module structure and vice-versa, so one does not talk about left or right R-modules when R is a commutative ring, only about R-modules. The usual facts apply to modules; for example, $-m = (-1_R)m$ and $0_R m = 0_M$. Here are some examples of modules. If R is a field, an R-module is called a *vector space.* If R is a division ring, a left R-module is called a *left vector space.* When $k \subseteq K$ are fields, then K is a k-vector space and so has a basis over k such that K is isomorphic (as a k-module) to a direct sum of copies of k; the number of copies is called the dimension of K over k. Similarly, when $R \subseteq S$ are division rings, S is a left R-vector space (also a right R-vector space, but never mind) and by the same proof as in the commutative case S has a left basis over R, so S is isomorphic (as a left R-module) to a direct sum of copies of R; the number of copies is called the dimension (or rank) of S over R.

M901, Assignment 6: Due Friday, November 11, 2011

Instructions: Do any three problems.

(1) Show that a group G of order $7^2 * 2^3$ is solvable.

(2) Let F be a finite field.

(a) Show that $\mathbf{Q}[x]$ has irreducible polynomials for every degree $d \geq 1$.

(b) Show that $F[x]$ has infinitely many irreducible polynomials (mimic Euclid's proof that $\mathbf{Z}$ has infinitely many primes); conclude for every integer d that $F[x]$ has an irreducible polynomial f of degree $\deg(f) \geq d$.

(3) A subgroup G of a group H is said to be a *characteristic* subgroup if for every automorphism f of H we have $f(G) = G$.

(a) Show that a characteristic subgroup is always normal.

(b) Show that the derived subgroups $H^{(i)}$ of a group H are characteristic subgroups (and hence normal).

(4) Let D be a division ring. For each $x \in D$, define the centralizer of x in D to be

$$C_D(x) = \{y \in D : yx = xy\}.$$

Define the center $Z(D)$ of D to be $\cap_{x \in D} C_D(x)$.

(a) Show that $C_D(x)$ is a division ring.

(b) Show that $Z(D)$ is a field.

(5) Let D be a division ring with finitely many elements. Let $x \in D$.

(a) Show that $|Z(D)| = q$ where $q = p^r$ for some prime p and some integer $r \geq 1$.

(b) Show that $|D| = q^s$ for some integer $s \geq 1$.

(c) Show that $|C_D(x)| = q^t$ for some integer $t \geq 1$ that divides s.

(d) Use the class equation applied to the group of non-zero elements of D to show that

$$q^s - 1 = (q - 1) + \sum_i \frac{q^s - 1}{q^{t_i} - 1}$$

for some positive integers t_i, each of which divides s.

(f) Look up and apply Zsigmondy's Theorem; conclude that either $s = 1$, or $s = 2$, or $q = 2$ and $s = 6$.

(g) Show that $s = 2$ is impossible. [Hint: if $s = 2$, pick a basis for D over $Z(D)$ and show explicitly that D is commutative, implying $s = 1$.]

(h) Show that $s = 6$ with $q = 2$ is impossible. [Hint: plug it into the displayed equation above.]

(i) Conclude that $s = 1$, so $D = Z(D)$, hence D is a field.