1. Let $G$ be a finite group, and let $N$ be a normal subgroup of $G$. Suppose that $H$ is a subgroup of $G$. Prove that the index $(H : (H \cap N))$ divides the index $(G : N)$. Deduce that if $H$ is a subgroup of $A_n$, then $(H : (H \cap A_n)) \leq 2$.

See problem 2(a) on the second midterm that the other class took. The group $H/(H \cap N)$ is a subgroup of $G/N$, so the order of the subgroup divides the order of the ambient group. The “Deduce” part comes from the choices $G = S_n$, $N = A_n$.

2. Write $(1\ 2)(1\ 2\ 3)(1\ 2\ 3\ 4)(1\ 2\ 3\ 4\ 5)$ as a product of disjoint cycles in $S_5$.

I presume that you all know how to do this. To check your work, do it again. Note that we compose from the right to the left; if you composed in the order order, you lost points.

3. Suppose that $G$ is a group of order $3825 = 3^2 \cdot 5^2 \cdot 17$.

   a. Show that $G$ has a unique subgroup $N$ of order 17.

The number of 17-Sylows divides $3^2 \cdot 5^2$ and is 1 mod 17. You can check, I hope, that 1 is the only divisor of $3^2 \cdot 5^2$ that is 1 mod 17.
b. Show that the group $N$ in part (a) is a subgroup of the center of $G$.

We have to show that the set of elements of $G$ that commute with all elements of $N$ is the entire group $G$. This set is the subgroup $C_G(N)$ of $G$. It contains $N$ because $N$ is cyclic, and therefore abelian. We need to show that its order is divisible by 9 and by 25; if so, its order will be divisible by the order of $G$ and we’ll be done. The arguments for 9 and for 25 are analogous. Take a 3-Sylow subgroup $T$ of $G$. To show that $T$ centralizes $N$ is to show that the action of $T$ on $N$ by conjugation is the trivial action. This action is given a priori by some homomorphism

$$
\phi : T \rightarrow \text{Aut } N,
$$

where $\text{Aut } N$ is the group of automorphisms of the group $N$. But $\text{Aut } N$ is isomorphic to $(\mathbb{Z}/17\mathbb{Z})^*$, which has order 16. Since 16 is prime to 9, $\phi$ must be the trivial homomorphism.

4. Let $R$ be a commutative ring with identity. When $n$ is an integer, write $n_R$ for the element of $R$ corresponding to $n$. For example, $3_R = 1 + 1 + 1$, where each “1” in the equation is the identity element of $R$. If $n$ and $m$ are relatively prime integers, show that the ideal $(n_R, m_R)$ in $R$ is all of $R$.

The point is that we can write $1 = an + bm$, where $a$ and $b$ are integers. (That’s basically what you should think of doing when someone tells you that a gcd is 1.) Then the ideal in question contains the $R$-element analogous to $an + bm$, which is the element 1 of $R$. An ideal containing 1 is the full ring $R$.

5. Suppose that $G$ is a finite group of $p$-power order (where $p$ is a prime number).

a. Let $A$ be a finite $G$-set (i.e., a set with an action of $G$). Prove the congruence $|A| \equiv |A^G|$ mod $p$, where $A^G$ is the set of elements of $A$ that are fixed by all elements of $G$.

The action of $G$ on $A$ divides $A$ into disjoint orbits. All orbits have $p$-power order. The orbits of size $> 1$ have sizes divisible by $p$. The orbits of size 1 consist of the fixed points. The congruence to be established (which is surely explained in the book) then follows.

b. Suppose that $N \neq \{1\}$ is a normal subgroup of $G$. Show that $N \cap Z(G)$ is not the trivial group.

Let $G$ act on $N$ by conjugation. The fixed set $N^G$ is the indicated intersection $N \cap Z(G)$. Its size is congruent mod $p$ to the number of elements of $N$, which is a power of $p$ bigger than 1. Hence the number of elements of $N \cap Z(G)$ is divisible by $p$. Accordingly, this intersection is not the trivial group.

6. Find the gcd of $11 + 7i$ and $18 + i$ in $\mathbb{Z}[i]$.

We can do this as in the Thursday “class” last week (RRR Week). The norms of these elements are 170 and 325; it’s pretty clear that gcd(170, 325) = 5. Hence the gcd of $11 + 7i$
and $18 - i$ has norm dividing 5, so it can be only one of the following three elements: 1, $2 + i$, $2 - i$ (up to units). Now $\frac{18 + i}{2 - i} = 7 + 4i$ and similarly $\frac{11 + 7i}{2 - i} = 3 + 5i$. Hence the gcd is $2 - i$.

See

http://math.stackexchange.com/questions/82350/gcd-of-gaussian-integers

for some perspective.

7. Let $R$ be a commutative ring with identity. Suppose that for each $a \in R$ there is an integer $n > 1$ such that $a^n = a$. Prove that every prime ideal of $R$ is a maximal ideal.

Let $P$ be a prime ideal of $R$. In the ring $R/P$, we still have the property that is “enjoyed” by $R$: for each $x \in R/P$, there is an $n \geq 2$ so that $x^n = x$. If $x$ is non-zero, we have $x^{n-1} = 1$ because $R/P$ is an integral domain. Then $x \cdot x^{n-2} = 1$, so that $x^{n-2}$ is an inverse to $x$. (Special case: if $n = 2$, then $x = 1$, and indeed $1 = x^{n-2}$ is an inverse to $x$.) We conclude that $R/P$ is a field—every non-zero element has an inverse—and that $P$ is maximal.