Dr. Martin Olbermann
Due: Wednesday, Apr. 9, in class

Math 114
Spring 2008

# Homework 10

**Proofs and explanations should always be written using complete English sentences.** You should always explain and justify each of the steps in your solution, unless otherwise noted. Write your name and "Math 114" on the top right of the first page.

**1. a)** Show that no group of order 20 is simple. (Use the Sylow theorems to find a normal subgroup.)

**b)** Show that no group of order 30 is simple. (Here the Sylow theorems do not uniquely determine the number of Sylow 3-subgroups and Sylow 5-subgroups. However assume that both of these numbers are different from 1. How many elements of order 3 and of order 5 would the group have?)

Solution:
a) If $G$ is a group of order 20, then the number of Sylow 5-subgroups is congruent to 1 modulo 5 and divides 20, so it must be 1. Hence there is a unique subgroup of order 5, and it must be normal. So $G$ is not simple.
b) If $G$ is a group of order 30, then the number of Sylow 5-subgroups is congruent to 1 modulo 5 and divides 30, so it must be 1 or 6. And the number of Sylow 5-subgroups is congruent to 1 modulo 3 and divides 30, so it must be 1 or 10. If there is a unique subgroup of order 3 or 5, it is normal and we are done. If not, there are 6 subgroups of order 5 and 10 subgroups of order 3. But all of these groups must be cyclic, so every non-trivial element of such a subgroup is a generator of the subgroup. It follows that no non-trivial element of $G$ is contained in more than one of these subgroups. But then we have at least $6 \cdot 4 + 10 \cdot 2$ elements in $G$, which is a contradiction.

**2. a)** Let $p$ be a prime number. Show that every group of order $p^2$ is abelian. (Use the fact that every finite $p$-group has a non-trivial center.)

**b)** Let $p$ and $q$ be distinct prime numbers. Show that every group of order $pq$ is soluble. (Find a normal subgroup using the Sylow theorems.)

Solution:
a) Let $G$ have order $p^2$. The center of $G$ is a non-trivial subgroup, so it has $p$ or $p^2$ elements. If it has $p^2$ elements, we are done. Suppose it has $p$ elements. Then it is cyclic, say generated by $a$. Let $b$ be a non-central element of $G$. But then $a, b$ generate $G$, and $b$ commutes with $a$ since $a$ is central. But $b$ also commutes with $b$. Hence $b$ commutes with all elements generated by $a, b$. So $b$ is central. Contradiction.
b) Let $G$ have order $pq$, and say $p < q$. The number of Sylow $q$-subgroups is congruent to 1 modulo $q$ and divides $p$. This number must be 1. So $G$ has a normal subgroup $H$ of order $q$. Then $1 \leq H \leq G$ is a series where the quotients are abelian groups. So $G$ is soluble.

**3.** Show that the Galois group of $t^p - 1$ over $\mathbb{Q}$ is isomorphic to the group $\mathbb{Z}_p^*$ of units of the ring $\mathbb{Z}_p$.

Solution:
We can consider the splitting field as the subfield $Q(\epsilon)$ of $\mathbb{C}$, where $\epsilon = e^{\frac{2\pi i}{p}}$. Then the degree of the field extension is $p-1$, since $t^{p-1} + t^{p-2} + \cdots + t + 1$ is irreducible over $\mathbb{Q}$. So the Galois group has $p-1$ elements. An element $\gamma$ is determined by its value on $\epsilon$, which is $\epsilon^k$, where $1 \leq k \leq p-1$. Mapping $\gamma$ to $k \in \mathbb{Z}_p^*$ defines an isomorphism between the Galois group and $\mathbb{Z}_p^*$.

**4.** Stewart, exercise 14.7.

Solution:
The zero expressible by radicals is contained in a radical extension $L$ of $K$. The other zeros are then contained in the normal closure of $L : K$, which is radical by Lemma 14.2.

**5.** Stewart, exercise 15.7.

Solution:
Apply an element $\tau$ of the Galois group to $T(a)$, you get $\tau\tau_1(a) + \cdots + \tau\tau_n(a)$. But the elements $\tau\tau_1, \ldots \tau\tau_n$ are also the $n$ elements of the Galois group. It follows that $\tau(T(a)) = T(a)$ for all $\tau$ in the Galois group, i.e. $T(a) \in \Gamma^{\#} = K$. Let $a \in K$, and let $b = a/n$. Then $T(b) = b + b + \cdots + b = a$, so $T$ is surjective on $K$.