Field Theory HW 2

Ali Nesin

October 2008

I. Given n let $\varphi(n) = |\{m = 1, ..., n : (m, n) = 1\}|$.

1. Show that $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

2. Show that $(n, m) = 1$ if and only if $\mathbb{Z}/nm\mathbb{Z} \approx \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as rings (so in particular as additive groups).

3. Conclude that that if $(n, m) = 1$ then $(\mathbb{Z}/nm\mathbb{Z})^* \approx (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ as groups.

4. Conclude that that if $(n, m) = 1$ then $\varphi(nm) = \varphi(n)\varphi(m)$.

5. Show that if p is a prime then for any positive natural number n, $\varphi(p^n) = p^n - p^{n-1}$.

6. Conclude that if $n = p_1^{n_1}...p_k^{n_k}$ then $\varphi(n) = (p_1^{n_1} - p_1^{n_1-1})...(p_k^{n_k} - p_k^{n_k-1})$.

7. Show that for all n, $n = \Sigma_{d|n}\, \varphi(d)$. (Hint: You may proceed by induction on n).

8*. Show that if K is a field and G a finite subgroup of K^* then G is cyclic. (Hint: Use above and proceed by induction to find an element of order $|G|$ of G. Use also the fact that in a field, the equation $X^d = 1$ has at most d roots.).

Now we will show the same result in a different way. (See II and III)

II. Let A be a group. For any prime p let $A(p) = \{a \in A : a^{p^k} = 1 \text{ for some } k\}$.

1. Show that if A is abelian then $A(p)$ is a characteristic subgroup of A. (The same holds if A is a nilpotent group but this is slightly more difficult to prove. See #V).

2. Show that if $a \in A$ is a torsion element then there are elements $a_p \in A(p)$ such that

i. $a_p = 1$ for almost all p.

ii. $a_pa_q = a_qa_p$ for all p and q.

iii. a is the product of all the a_p.

(Hint: You may choose each a_p a suitable power of a)

3. Conclude that if A is a torsion abelian group then $A = \oplus_p A(p)$. (The same holds if A is a nilpotent group but this is slightly more difficult to prove).

III. Let K be a field and G a finite subgroup of K^*. We want to show that G is cyclic.

1. Show that it is enough to show this in case G is a p-group for a prime p.

2. Show that G is a cyclic group. (Hint: In a field the equation $X^n = 1$ has at most n roots.)

IV. We push farther and generalize #II.

Let p be a prime and A an abelian group of exponent p^n.

1. Let $a \in A$ be an element of order p^n. Show that $A = \langle a \rangle \oplus C$ for some subgroup C of A.

2. Conclude that if A is finite then A is a direct product of cyclic groups.

3*. Let B be a subgroup of A isomorphic to $\oplus\, \mathbb{Z}/p^n\mathbb{Z}$. Show that $A = B \oplus C$ for some subgroup C of A. (Hint: In case A is infinite you have to use Zorn's Lemma).

4*. Conclude that A is a direct sum of cyclic groups.

V. We push farther and generalize #IV. Let G be a group and p a prime.

1. Show that G has maximal p-subgroups. (Zorn's Lemma).

2. Suppose G is a nilpotent group. Show that for any $H < G$, $H < N_G(H)$. (Hint: By induction on the nilpotency class of G).

3. Conclude that if G is a nilpotent group and H is a maximal p-subgroup of G then H is characteristic in $N_G(H)$.
4. Conclude from 2 and 3 that if H is a maximal p-subgroup of G then H is normal in G. (Hint: $N_G(N_G(H))$ acts on $N_G(H)$ and it leaves invariant H).
5. Conclude that a nilpotent group has a unique maximal p-subgroup.
5. Conclude that a torsion nilpotent group is a direct sum of its maximal p-subgroups for prime p.