**Problem assignment 7.5**

**Representations of Finite Groups.**

Joseph Bernstein May 10, 2007.

**Brauer's Induction Theorem.**

Here I will give a proof of Brauer induction theorem.

In the proof I use several lemmas (lemmas 1 - 5) which are pretty standard. I leave them, as exercises.

**Definition**. Let $p$ be a prime number. A finite group $E$ is called **p-elementary** if is it is isomorphic to a direct product of a cyclic group $C_m$ of order $m$ prime to $p$ and a $p$-group $S$.

**Lemma 1.** Show that a subgroup of an elementary group is elementary.

Fix a finite group $G$ and denote by $R(G)$ its character ring. We will prove

**Brauer Induction Theorem.** The group $R(G)$ is spanned by representations of the form $Ind_E^G(\chi)$, where $E \subset G$ is an elementary subgroup and $\chi$ a one dimensional representation of $E$.

**Proof.**

**Step 1.** Set $I(G) = \sum_E Ind_E^G(R(E) \subset R(G)$. It is enough to prove

**Statement 1.** $I(G)$ contains the element $1 = \mathbf{1}_G$.

Indeed, from projection formula it is clear that $I(G)$ is an ideal of $R(G)$. If it contains 1 it coincides with $R(G)$.

On the other hand, for an elementary group $E$ any irreducible representation $\rho$ is induced from a character of some subgroup $E'$ since $E$ is nilpotent.

Since $E'$ is elementary this shows that $R(E)$ is spanned by representations induced from characters of elementary subgroups, and hence $R(G) = I(G)$ is spanned by such induced characters.

For every finite group $H$ let $C(H)$ denote the space of complex valued functions on $H$ invariant under conjugation. $C(H)$ is an algebra with respect to multiplication. For any subgroup $D \subset H$ we have restriction and induction morphisms $Res_H^D : C(H) \to C(D)$ and $Ind_D^H : C(D) \to C(H)$.

**Definition**. A character system $Q$ is a correspondence which assigns to every finite group $H$ a subgroup $Q(H)$ of the space $C(H)$ such that these subgroups are closed with respect to multiplication, restriction and induction.

**Examples.**

(i) $Q(H) = R(H)$. Here we identify $R(H)$ with a subgroup $\mathcal{C}h(H) \subset C(H)$ using the morphism $\pi \mapsto ch(\pi)$.

(ii) $Q(H) = C(H)$.

(iii) $Q(H) = C_{\mathbf{Z}}(H)$, the subgroup of integer valued functions.

**Step 2.** Let $n = \#(G)$, $\mu_n \subset \mathbf{C}$ be the group of $n$-th roots of 1. Let $\Lambda$ denote subring of $\mathbf{C}$ generated by $\mu_n$.

Consider the character system $R_\Lambda$ defined by $R_\Lambda(H) = \Lambda \cdot R(H) \subset C(H)$. As before, we set $I_\Lambda(G) = \sum_{E \subset G} Ind_E^G(R_\Lambda(E))$.

It is enough to prove

**Statement 2.** $1 \in I_\Lambda(G)$.

In order to see that **Statement 2.** implies **Statement 1.** we will use the following

**Lemma 2.** There exists a homomorphism of groups $\nu : \Lambda \to \mathbf{Z}$ such that $\nu(1) = 1$.

Notice that for any group $H$ there exists unique morphism of groups $\nu = \nu_H : R_\Lambda(H) \to R(H)$ such that $\nu(\lambda r) = \nu(\lambda)r$ for $\lambda \in \Lambda$ and $r \in R(H)$. This is true since $R(H)$ has a basis $\{\rho_1, ..., \rho_r\}$ of irreducible representations which stays a basis in $C(H)$.

Clearly the system of morphisms $\nu_H$ is compatible with restriction and induction. In particular, this implies that $\nu(I_\Lambda(G)) \subset I(G)$.

Now if we know that $1 \in I_\Lambda$ we get that $1 = \nu(1) \in \nu(I_\Lambda) \subset I$.

**Step 3.** Consider the character system $Q(H) = R_\Lambda(H) \bigcap C_{\mathbf{Z}}(H)$, i.e. we consider all functions $f \in R_\Lambda(H)$ that take only integer values. Consider the ideal $J = \sum_{E \subset G} Ind_E^G(Q(E))$. Our aim is to prove

**Statement 3.** $1 \in J$

**Step 4.** It is enough to prove the following

**Statement 4.** For any prime number $p$ and any integer $N$ we have $1 \in J(mod p^N)$, i.e. $1 \in J + p^N C_{\mathbf{Z}}(G)$.

The fact that statement 4 implies statement 3 follows from the following general

**Lemma 3.** Let $L$ be a lattice, i.e. a group isomorphic to $\mathbf{Z}^r$. Consider a tower of subgroups $A \subset B \subset L$. Then in order to show that $A = B$ it is enough to check that $A \equiv B(mod\ p^N)$ for all primes $p$ and all integers $N$ (here $A \equiv B(mod\ p^N)$ means $A + p^N L = B + p^N L$).

**Step 5.** Fix a prime number $p$ and show that the statement 4 holds for powers of $p$. In fact in order to do this it is enough to show much weaker

**Statement 5.** There exists a function $f \in J$ such that for every element $g \in G$ its value $f(g)$ is prime to $p$.

Indeed, suppose we found such function $f$. Then the function $f_1 = f^{p-1}$ lies in $J$ since $J$ is an ideal and it satisfies $f_1 \equiv 1\ (mod\ pC_{\mathbf{Z}}(G))$.

Now we recursively define a sequence of functions $f_1, f_2, ... \in J$ by $f_{k+1} = f_k^p$ and see that $f_k \equiv 1\ (mod\ p^k C_{\mathbf{Z}}(G))$, which proves the statement 4.

**Step 6.** Fix a prime number $p$. An element $g$ of a finite group $G$ is called **p-regular** if $ord(g)$ is prime to $p$ and it is called **p-singular** if $ord(g)$ is a power of $p$.

Let us remind the following standard

**Lemma 4.** (Jordan decomposition). (i) Let $G$ be a finite group. Every element $g \in G$ can be uniquely written as $g = g_r g_s$, where $g_r$ and $g_s$ are commuting p-regular and p-singular elements of $G$.

These elements are called p-regular and p-singular parts of $g$.

Let us note that the uniqueness in the Jordan decomposition implies that the maps $g \mapsto g_r$ and $g \mapsto g_s$ are compatible with morphisms of groups. In particular, they map conjugacy classes into conjugacy classes.

**Step 7.** It is enough to prove the following

**Statement 7.** Let $a \in G$ be a p-regular element. Then there exists a function $f_a \in J$ such that $f_a(x) = 0$ if element $x_r$ is not conjugate to $a$ and $f_a(x)$ is prime to $p$ if $x_r$ is conjugate to $a$.

Indeed, it is clear that the function $f$ which is a sum of functions $f_a$ over representatives $a$ of p-regular conjugacy classes satisfies conditions of statement 5.

**Step 8. Proof of statement 7.** So now we fixed a prime number $p$ and a p-regular element $a \in G$.

Set $m = ord(a)$ and denote by $D$ the cyclic subgroup generated by $a$. Let us denote by $C(a)$ the centralizer of the element $a \in G$.

Let us fix a $p$-Sylov subgroup $S$ of the group $C(a)$ and set $E = D \times S \subset C(a)$.

It is easy to see that $E$ is an elementary subgroup and the projection $p : E \to D$ coincides with the map $x \mapsto x_r$.

Consider the function $\phi \in C(E)$ defined by $\phi(x) = 0$ if $p(x) \neq a$ and $\phi(x) = m$ if $p(x) = a$.

**Claim.** (i) $\phi \in Q(E)$

(ii) The function $f_a = Ind_E^G(\phi)$ satisfies the conditions of statement 7.

**Proof of claim**.

(i) Function $\phi$ takes integer values. Also we can write it in the form $\phi = \sum_\chi \chi(a^{-1}) \cdot \chi'$, where the sum is taken over all characters $\chi$ of the group $D$ and $\chi'$ is the character of the group $E$ defined by $\chi'(x) = \chi(p(x))$.

Since coefficients $\chi(a^{-1})$ lie in $\Lambda$ we see that $\phi \in R_\Lambda(E)$, i.e. $\phi \in Q(E)$.

(ii) This is a straightforward computation. By definition

(*) $f_a(x) = \sum_{g \in G/E} \phi_!(g^{-1}xg)$, where

$\phi_!$ is the extension by 0 of the function $\phi$ to $G$.

Let $x \in G$. If $x_r$ is not conjugate to $a$ then all the terms in the sum are 0 since the function $\phi_!$ is supported on elements which regular part equals $a$.

Assume now that $x_r$ is conjugate to $a$. By conjugating we can assume that $x_r = a$.

Let us write Jordan decomposition $x = at$, where $t = x_s$. It is clear that $t \in C(a)$.

It is clear that in the sum (*) above non-zero contribution is given only by terms $g$ such that $(g^{-1}xg)_r$ equals to $a$. Since $(g^{-1}xg)_r = g^{-1}x_rg = g^{-1}ag$ this means that $g \in C(a)$. Thus we have

(**) $f_a(x) = \sum_{g \in C(a)/E} \phi_!(g^{-1}xg)$,

Let us denote the set $C(a)/E$ by $Y$ and consider the subset

$Z = \{g \in Y | g^{-1}tg \in S\}$.

It is clear from the formula (**) that $f_a(x) = m \cdot \#(Z)$.

We want to show that this number is prime to $p$.

Note that an element $g \in Y$ belongs to $Z$ iff $g^{-1}tg \in E$ , i.e. $tg \in gE$. In other words this is equivalent to the condition that $y$ is a fixed point of the left action of $t$ on $Y$. Since the size of $Y$ is prime to $p$ this follows from the following general

**Lemma 5.** Let $t$ be a p-regular transformation of a finite set $Y$ and $Z \subset Y$ be the subset of its fixed points. Then $\#(Z) \equiv \#(Y)$ $(mod\ p)$.