Brauer Characters and Green's Theorem

February 12, 2004

1 The Jacobson Density Theorem

We will review without proof some standard results on semisimplicity.

If R is a ring, an R-module M is *simple* or *irreducible* if $M \neq 0$ but M has no proper nontrivial submodules. It is *semisimple* if any one of the following three equivalent conditions are satisfied.

- M is a sum of simple submodules;
- M is a direct sum of simple submodules;
- If $N \subseteq M$ is a submodule, there exists another submodule N' such that $M = N \oplus N'$.

The equivalence of these three conditions is proved in Lang's *Algebra*, p. 645. The equivalence of the second two conditions, which is enough for our purposes, is proved in Rotman's *Advanced Modern Algebra*, Proposition 8.42 on p. 552.

Suppose that M is an R-module. Then M is an abelian group, and we have a ring homomorphism $\mu : R \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ defined by $rm = \mu(r)m$. Conversely, given a ring R and an abelian group M, and a ring homomorphism $\mu : R \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$, the rule $rm = \mu(r)m$ makes M into an R-module.

This simple observation leads to the following considerations. Let A be the subring of $\mathrm{End}_{\mathbb{Z}}(M)$ which commutes with the image of μ. The ring A is called the *commuting ring* of R. The inclusion $A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ makes M into an A-module. Any element of A is of course an R-module endomorphism of M, so in fact $A = \mathrm{End}_R(M)$. Now we may consider the commuting ring $\mathrm{End}_A(M)$. It is clear that the image of μ is contained in $\mathrm{End}_A(M)$.

Theorem 1 (Jacobson Density Theorem) *Let R be a ring and M a semisimple R-module. Let $A \in \mathrm{End}_{\mathbb{Z}}(M)$ be the commuting ring of R. If $f \in \mathrm{End}_A(M)$, and if $x_1, \cdots, x_n \in M$, then there exists $r \in R$ such that $rx_i = f(x_i)$.*

Proof See Lang's *Algebra*, Theorem 3.2 on p. 647. $\square$

Remark 1 In the applications, R will be a finite-dimensional algebra over a field F, and M will be finite-dimensional as an F-vector space. In that case, we may take x_i to be a basis of M, and the conclusion of the density theorem can be stated simply that $\mu : R \longrightarrow \mathrm{End}_A(M)$ is surjective.

2 Splitting Fields

We recall that if F is a field then a representation $\pi : G \longrightarrow \mathrm{GL}(n, F)$ is *absolutely irreducible* if the representation $\mathrm{GL}(n, E)$ is irreducible for every extension E of F. We call the subring of $\mathrm{Mat}_n(F)$ commuting with $\pi(G)$ the *commuting ring* of π. It is of course commuting ring of the subalgebra of $\mathrm{Mat}_n(F)$ generated by $\pi(G)$.

Lemma 1 *Let A be a finite-dimensional algebra over a field F such that $E \otimes_F A$ is a division ring for all extensions E of F. Then $A = F$.*

Proof If $x \in A$, then $F[x]$ is a field since it is a commutative subring of a division algebra. $E \otimes_F F[x]$ is a commutative subring of $E \otimes_F A$ for all extensions E of F. In particular, taking E to be the algebraic closure of F, $E \otimes_F F[x]$ is a field which is a finite extension of E, hence $E \otimes_F F[x] = E$, which means that $x \in F$. $\square$

Proposition 1 *Let $\pi : G \longrightarrow \mathrm{GL}(n, F)$ be a representation of the finite group G, and let $\Lambda \subseteq \mathrm{Mat}_n(F)$ be the commuting ring of π.*

(i) If π is irreducible, then Λ is a division ring. If the characteristic of F is zero, or a prime not dividing $|G|$, then the converse is true: Λ being a division ring implies the irreducibility of π.

(ii) If π is irreducible and then π is absolutely irreducible if and only if Λ is the center of $\mathrm{Mat}_n(F)$, consisting of scalar matrices. The assumption that π is irreducible is unnecessary if the characteristic of F is zero, or a prime not dividing $|G|$.

(iii) If F is algebraically closed then every irreducible representation is absolutely irreducible.

Proof For (i), if $A \in \mathrm{Mat}_n(F)$ commutes with $\pi(G)$, and if π is irreducible, then the kernel of A is an invariant subspace, hence by Schur's Lemma it is trivial unless $A = 0$. Thus A is zero or invertible. Therefore the commuting ring is a division ring. Conversely if π is reducible, and W is a proper, nontrivial invariant subspace of F^n, let $P : F^n \longrightarrow W$ be any projection map. Assuming that $|G|$ is invertible in F, we may replace P by $|G|^{-1} \sum \pi(g) \circ P \circ \pi(g)^{-1}$. This means that if the characteristic of F is zero, or a prime not dividing $|G|$ we may assume that P is G-equivariant. The matrix representing the endomorphism P has determinant zero, and is in Λ, so Λ is not a division ring.

Assuming that π is irreducible, F^n is a simple $F[G]$-module with the action induced by the representation $\pi : G \longrightarrow \mathrm{End}(F^n) = \mathrm{Mat}_n(F)$. Hence we may use the Jacobson density theorem. If the commuting ring Λ is the field of scalar matrices, then by the density theorem, $\pi(G)$ spans $\mathrm{Mat}_n(F)$, which is the commuting ring of Λ. Consequently $\pi(G)$ spans $\mathrm{Mat}_n(E)$ as an E-vector space for any extension field, which clearly implies that $\pi(G)$ is irreducible as a representation over E. If $|G|$ is invertible in F, then by (i) the assumption that Λ consists of scalar matrices implies that π is irreducible, so we may omit the assumption of irreducibility.

Part (iii) follows since any division algebra D over an algebraically closed field F is F itself. $\square$

The field F is called a *splitting field* for G if every irreducible representation of G over F is absolutely irreducible.

We recall that if R is a ring and M an R-module, then *composition series* consists of a sequence $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_k = M$ such that M_{i+1}/M_i are simple. According to the *Jordan-Hölder Theorem*, the quotients M_{i+1}/M_i are independent of the choice of composition series. They are called the *composition factors* of M. Not every

Proposition 2 *Let G be a finite group and F a splitting field for G. Assume that the characteristic of F is not a prime dividing $|G|$. If $E \supset F$ is any bigger field, then any irreducible representation $\varphi : G \longrightarrow \mathrm{GL}(n, E)$ is equivalent to a representation $G \longrightarrow \mathrm{GL}(n, F)$.*

Proof Let V be an irreducible $E[G]$-module corresponding to the representation φ of G. Picking a nonzero element v of V, let $\psi : E[G] \longrightarrow V$ be the map $\psi(r) = rv$. This is an $E[G]$-module homomorphism, so V is a quotient of $E[G]$. Since it is simple, it is therefore a composition factor of $E[G]$.

Now let $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_k = F[G]$ be a composition series for $F[G]$. Then $0 = EM_0 \subset EM_1 \subset EM_2 \subset \cdots \subset EM_k = E[G]$ can be refined to a composition series for $E[G]$, and by the Jordan-Hölder Theorem V must isomorphic to a composition factor of one of the quotients $EM_{i+1}/EM_i \cong E \otimes (M_{i+1}/M_i)$. But M_{i+1}/M_i is absolutely irreducible since F is a splitting field, so φ is equivalent to the representation of F on M_{i+1}/M_i. $\square$

3 Valuation Rings

Let F be a field. A *valuation ring* of F is a commutative integral domain R whose field of fractions is F, such that if $x \in F$ either $x \in R$ or $x \neq 0$ and $x^{-1} \in R$.

Proposition 3 *A valuation ring R is a local ring. Its maximal ideal $\mathfrak{m}$ consists of the nonunits of R. It is integrally closed in its field of fractions.*

Proof To show that R is a local ring it is enough to show that the nonunits form an ideal $\mathfrak{m}$, since any proper ideal must be contained in the nonunits.

It is clear that if $u \in \mathfrak{m}$ and $r \in R$ then $ru \in \mathfrak{m}$.

If $u, v \in \mathfrak{m}$ we show $u + v \in \mathfrak{m}$. There is nothing to show if u or v is zero. Otherwise, either u/v or v/u is in R. Assume that $u/v \in R$. Then $(u+v)/v = 1+u/v \in R$. If $u+v$ is a unit, then $1/v \in R$ which is a contradiction since v is a nonunit. Thus $u + v \in \mathfrak{m}$.

We have proved that R is a local ring. To see that it is integrally closed in its field of fractions F, suppose that $u \in F$ satisfies a relation of integral dependence over F:

$$u^n + a_{n-1}u^{n-1} + \ldots + a_0 = 0, \qquad a_i \in R.$$

If $u \notin R$ then $u^{-1} \in \mathfrak{m}$. Writing

$$1 = -(a_{n-1}u^{-1} + \ldots + a_0 u^{-n})$$

gives a contradiction since the right hand side is in $\mathfrak{m}$. $\square$

Theorem 2 *Let F be a field, and let K be an algebraically closed field. Let A be a subring of F and let $\varphi : F \longrightarrow K$ be a homomorphism. Then there exists a valuation ring R of F containing A such that φ can be extended to a homomorphism of $R \longrightarrow K$. The kernel of this extension is the maximal ideal of R.*

This theorem in commutative algebra (due to van der Waerden) is extremely handy in algebraic geometry.

Proof Let Σ be the set of all ordered pairs (R, Φ), where R is a subring of F containing A, and Φ is an extension of φ to a homorphism $R \longrightarrow K$. Order Σ by $(R_1, \Phi_1) \leqslant (R_2, \Phi_2)$ if $R_1 \subseteq R_2$ and if the restriction of Φ_2 to R_1 is Φ_1. By Zorn's Lemma, Σ has maximal elements. Let (R, Φ) be a maximal element of Σ.

Let us show that R is a local ring. Let $\mathfrak{m} = \ker(\Phi)$. If $x \in R - \mathfrak{m}$, we will show that x is a unit. This is enough since it implies that the nonunits of R comprise the ideal $\mathfrak{m}$, which is therefore the unique maximal ideal. Since $\Phi(x) \neq 0$, let $\xi = \Phi(x)^{-1} \in K$. We can define a homomorphism $\Phi_1 : R[x^{-1}] \longrightarrow K$ by

$$\Phi_1 \left(\sum_{k=0}^{N} a_k x^{-k} \right) = \sum_{k=0}^{N} \Phi(a_k) \xi^k.$$

To check that this is well-defined, if $\sum a_k x^{-k} = 0$ we have $\sum a_k x^{N-k} = 0$, where now the exponents are positive. Applying Φ, $\sum \Phi(a_k) \xi^{-(N-k)} = 0$, which implies that $\sum \Phi(a_k) \xi^k = 0$. Thus Φ_1 is well-defined. Using the maximality of (R, Φ) we see that $R[x^{-1}] = R$ so $x^{-1} \in R$ and thus x is a unit.

If $x \in F$ we must show that either $x \in R$ or $x^{-1} \in R$. Let $\mathfrak{m} = \ker(\Phi)$ be the maximal ideal of R. Let $R_1 = R[x]$ and $R_2 = R[x^{-1}]$. We claim that either $\mathfrak{m}R_1$ or $\mathfrak{m}R_2$ is a proper ideal. If not, we have relations

$$1 = m_0 + m_1 x + \ldots + m_r x^r = m_0' + m_1' x^{-1} + \ldots + m_s' x^{-s},$$

where the m_i and m_i' are in Φ. We assume that the degrees r and s are chosen as small as possible. Without loss of generality we may assume that $s \leqslant r$. Now

$$1 - m_0' = m_1' x^{-1} + \ldots + m_s' x^{-s},$$

and this is a unit since $m_0' \in \mathfrak{m}$. We may multiply this relation by $(1 - m_0')^{-1} m_r x^r$ and substitute the resulting expression for $m_r x^r$ into the first relation, reducing the degree. This is a contradiction.

By symmetry, we may assume that $\mathfrak{m}R_1$ is a proper ideal, and show that Φ can be extended to R_1. This will imply our claim that R is a valuation ring since using the maximality of (R, Φ) is Σ, this will show that $R_1 = R$, so that $x \in R$. First note that x is algebraic over the field of fractions of R, since otherwise we could extend Φ to R_1 by mapping x arbitrarily, contradicting the maximality of (R, Φ). Let $\mathfrak{m}_1$ be a maximal ideal of R_1 containing $\mathfrak{m}R_1$. Then $\mathfrak{m}_1 \cap R \supseteq \mathfrak{m}$, and by maximality of $\mathfrak{m}$ we have $\mathfrak{m}_1 \cap R = \mathfrak{m}$. Thus $R_1/\mathfrak{m}_1$ is an algebraic field extension of $R/\mathfrak{m}$, which is isomorphic to a subfield of the algebraically closed field K. Hence $R_1/\mathfrak{m}_1$ is isomorphic to a subfield of K, and the composition $R_1 \longrightarrow R_1/\mathfrak{m}_1 \longrightarrow K$ is an extension of Φ. $\square$

Proposition 4 *Let F be a field and R a valuation ring of F, with maximal ideal $\mathfrak{m}$. If $x_1, \cdots, x_n$ are elements of F, not all zero, then there exists an element $\beta \in F^\times$ such that $\beta x_i \in R$, and not all βx_i are in $\mathfrak{m}$.*

Proof Define an order on $F^\times$, in which $x \leqslant y$ if $y/x \in R$. Since R is a valuation ring, this is a total order. We can take $\beta = x_j^{-1}$ where x_j is minimal with respect to this order. $\square$

4 Brauer Characters

Let p be a prime, which will be fixed. Let K be the algebraic closure of $\mathbb{F}_p$. Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Let R be a valuation ring of $\bar{\mathbb{Q}}$, with $\varphi : R \longrightarrow K$ extending the canonical map $\mathbb{Z} \longrightarrow \mathbb{F}_p$. Let $U \subset \mathbb{C}$ be the group of roots of unity of order prime to p. Any element of $\varepsilon \in U$ must lie in R (since otherwise $\varepsilon^{-1} \in R$, and ε is a power or ε^{-1}.) If $(p, m) = 1$ then both U and $K^\times$ contain exactly $\phi(m)$ primitive m-th roots of unity, where ϕ is Euler's totient, and U and $K^\times$ are exhausted by these as m runs though the integers, so φ must map the group U isomorphically onto $K^\times$. The inverse map to this isomorphism is a character $\theta : K^\times \longrightarrow U$.

Let G be a finite group. An element $g \in G$ is called *p-regular* if $p \nmid |g|$. It is called *p-singular* if its order is a power of p. If V is a finite-dimensional vector space over K, and $\rho : G \longrightarrow \mathrm{GL}(V)$ is a representation, then the *Brauer character* φ_ρ of ρ is a complex-valued function on the p-regular elements of G. If $g \in G$ is p-regular, and the eigenvalues of g are $\alpha_1, \cdots, \alpha_d$, then $\varphi_\rho(g) = \sum \theta(\alpha_i)$.

Theorem 3 *Let (π, V) be a complex representation of a finite group with ordinary character χ. Then π is equivalent to a matrix representation $\pi_1 : G \longrightarrow \mathrm{GL}(n, R)$ taking values in the valuation ring R. Let $\rho : G \longrightarrow \mathrm{GL}(n, K)$ be the composition with the canonical map $\mathrm{GL}(n, R) \longrightarrow \mathrm{GL}(n, K)$. If g is p-regular, then $\varphi_\rho(g) = \chi(g)$.*

Proof The field of fractions of R is the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. It is a splitting field for G, so π is equivalent to a representation $\pi_0 : G \longrightarrow \mathrm{GL}(n, \bar{\mathbb{Q}})$. Let $v_1, \cdots, v_n$ be a basis of $\bar{\mathbb{Q}}^n$. Let L be the R-submodule of $\bar{\mathbb{Q}}^n$ spanned by the $\pi(g)v_i$ for $g \in G$. Then $\bar{L} = L/\mathfrak{m}L$ is a finite-dimensional vector space over

$K = R/\mathfrak{m}R$. Let $\overline{w}_1, \cdots, \overline{w}_r$ be a basis, and let $w_1, \cdots, w_r$ be elements of L whose images span $\bar{L}$.

We show that $w_1, \cdots, w_r$ are linearly independent over $\bar{\mathbb{Q}}$. If not, let $\sum_i a_i w_i = 0$, where the $a_i \in \bar{\mathbb{Q}}$. By Proposition 4, we may assume that the $a_i \in R$ and not all $a_i \in \mathfrak{m}$. If $\overline{a_i} \in K$ are their images modulo $\mathfrak{m}$, we have $\sum \bar{a}_i \bar{w}_i = 0$, contradicting the linear independence of the $\overline{w_i}$.

Let L' be the R-submodule of $\bar{\mathbb{Q}}^n$ spanned by $w_1, \cdots, w_r$. We have $L' + \mathfrak{m}L = L$, which means that $\mathfrak{m}(L/L') = (L' + \mathfrak{m}L)/L' = (L/L')$. By Nakayama's Lemma, it follows that $L/L' = 0$. Therefore $L = Rw_1 + \ldots + Rw_r$. Since L contains the basis $v_1, \cdots, v_n$ of $\bar{\mathbb{Q}}^n$, we see that the w_i span $\bar{\mathbb{Q}}^n$. Thus $r = n$ and $w_1, \cdots, w_n$ are a basis of $\bar{\mathbb{Q}}^n$. With respect to this basis, $\pi_0(g)$ is represented by an $n \times n$ matrix $\pi_1(g)$ with coefficients in R.

Now suppose that g is p-regular. The characteristic polynomial f of $\pi_1(g)$ has its roots $\alpha_1, \cdots, \alpha_n$ in U, since g is p-regular. If $\bar{\alpha}_1, \cdots, \bar{\alpha}_n$ are the images of these in K, then $\theta(\bar{\alpha}_i) = \alpha_i$. Of course the $\overline{\alpha_i}$ are the eigenvalues of $\rho(g)$, so $\varphi_\rho(g) = \sum \theta(\bar{\alpha}_i) = \chi(g)$. □

Corollary 1 *Let (π, V) be a complex representation of a finite group with ordinary character χ. Then the restriction of χ to the p-regular elements is a Brauer character.*

If $g \in G$, we may write $g = g_p \cdot g_{p'}$ where g_p and $g_{p'}$ are suitable powers of g (hence commute) and g_p is p-singular while $g_{p'}$ is p-regular.

Proposition 5 *Let $\rho : G \longrightarrow \mathrm{GL}(d, K)$ be a representation. Let $\psi : G \longrightarrow K$ be its character, so $\psi(g) = \mathrm{tr}\ \rho(g)$. Then $\psi(g) = \psi(g_{p'})$.*

Proof After a change of basis we may assume that $\rho(g)$ is upper triangular. Then g_p is of prime power order and upper triangular, so its eigenvalues are 1. Multiplying $g_{p'}$ by g_p does not change its diagonal entries or its trace. □

Proposition 6 *Let $V_1, \cdots, V_h$ be representatives of the irreducible representations of G over K, and let φ_i be the corresponding Brauer characters. Then the φ_i are linearly independent.*

Proof Let $\pi_i : G \longrightarrow \mathrm{GL}(d_i, K)$ be the irreducible representations of G affording the Brauer characters φ_i. We let $V_i = K^{d_i}$ with the $K[G]$-module structure corresponding to the representation π_i. We also let $\psi_i : G \longrightarrow K$ be the characters of the representations, so $\psi_i(g) = \mathrm{tr}\ \pi_i(g)$.

Suppose that the φ_i are linearly dependent over $\mathbb{C}$. Since they are functions on G taking values in $\bar{\mathbb{Q}}$, they are linearly dependent over $\bar{\mathbb{Q}}$. By Proposition 4, there exist $\alpha_i \in R$ such that some α_i, say α_1 is not in $\mathfrak{m}$ and $\sum \alpha_i \varphi_i = 0$. Now if g is p-regular, applying the canonical map $R \longrightarrow K$ gives the relation $\sum \overline{\alpha_i} \psi_i(g) = 0$, where the $\bar{\alpha}_i$ are the images of the α_i in R. By Proposition 5, the equality $\sum \bar{\alpha}_i \psi_i(g) = 0$, proved for g p-regular, is true for all g.

Now consider the direct sums of the representations π_i. Since the π_i are mutually nonisomorphic, any $K[G]$-module endomorphism of $\bigoplus V_i$ must map

V_i to itself, and by Schur's Lemma it is a scalar on V_i. Thus the commuting ring Λ of $\oplus\pi_i$ is $\bigoplus_i F$ embedded by block scalar matrices in $\bigoplus \mathrm{Mat}_{d_i}(F)$. Let $f_1 : V_1 \longrightarrow V_1$ be any linear transformation with nonzero trace. By the Jacobson density theorem, which is applicable because $\bigoplus V_i$ is a semisimple $K[G]$-module, there exists $\sum c_i g_i \in K[G]$ which induces f_1 on V_1, and 0 on the other constituents, since the linear transformation we have described commutes with Λ. Now $0 = \sum_{i,j} c_j \alpha_i \psi_i(g_j) = \alpha_1 \,\mathrm{tr}(f_1) \neq 0$, which is a contradiction. $\square$

Theorem 4 *The number of irreducible representations of G over F is equal to the number of p-regular conjugacy classes.*

Proof By Proposition 6, the number of irreducible representations is equal to the number of linearly independent Brauer characters. The Brauer characters are class functions defined only on the p-regular conjugacy classes, and any restriction of an ordinary character to the p-regular conjugacy classes is a Brauer character. By Schur orthogonality there are enough of these to separate the conjugacy classes, and the result follows. $\square$

Theorem 5 *Suppose that $p \nmid |G|$. Then the Brauer characters of the irreducible representations of G over K are the same as the characters of the irreducible representations of G over $\bar{\mathbb{Q}}$.*

Proof Let χ_i be the irreducible characters of G over $\bar{\mathbb{Q}}$, and φ_i the irreducible Brauer characters of G over K. Then $\chi_i(1)$ are the character degrees, so $\sum_i \chi_i(1)^2 = |G|$.

Since the characteristic of K is prime to p, the group ring $K[G]$ is semisimple, and since K is algebraically closed, it is a splitting field. The φ_i are the degrees of the irreducible representations of G over K, so we have also $\sum_i \varphi_i(1)^2 = |G|$.

By Theorem 3 each χ_i may be expressed in terms of the φ_i, so we may write

$$\chi_i = \sum_j d_{ij}\varphi_j, \qquad 0 < d_{ij} \in \mathbb{Z}. \tag{1}$$

Squaring this and summing,

$$\sum_j \varphi_j(1)^2 = |G| = \sum_i \chi_i(1)^2 = \sum_i \left(\sum_j d_{ij}\varphi_j(1)\right)^2 =$$
$$\sum_j \left(\sum_i d_{ij}^2\right)\varphi_j(1)^2 + \sum_{j<k}\sum_i d_{ij}d_{ik}\varphi_j(1)\varphi_k(1).$$

Thus

$$\sum_j \left[\left(\sum_i d_{ij}^2\right) - 1\right]\varphi_j(1)^2 + \sum_{j<k}\sum_i d_{ij}d_{ik}\varphi_j(1)\varphi_k(1) = 0.$$

We note that for each i, at least one d_{ij} is nonzero. Indeed, the square matrix (d_{ij}) must be invertible since both the χ_i and the φ_i are bases for the spaces of class functions. Thus every term on the left side of our last identity is non-negative, so they are all zero. This implies that for each j, exactly one d_{ij} is nonzero, and that $d_{ij} = 1$. Rearranging the φ_j if necessary, we have $\varphi_i = \chi_i$. □

5 Green's Theorem

We recall Brauer's well-known characterization of characters. If l is a prime, an *l-elementary group* is one of the form $C \times L$, where C is a cyclic group of order prime to l, and L is an l-group.

Theorem 6 *Suppose that $\chi : G \longrightarrow \mathbb{C}$ is a class function on the finite group G. If the restriction of χ to every elementary subgroup is a generalized character.*

This is proved in Lang's *Algebra*, Corollary 10.12 on p. 709. Proofs may also be found in most books on Group Representation Theory.

Theorem 7 *Let G be a finite group, and let $\rho : G \longrightarrow \mathrm{GL}(n, \mathbb{F}_q)$ be a representation of G. Let S be a symmetric polynomial with integer coefficients. Let $\theta : \bar{\mathbb{F}}_q^\times \longrightarrow \mathbb{C}^\times$ be a character. Let*

$$\chi(g) = S(\theta(\alpha_1), \cdots, \theta(\alpha_n)),$$

where α_i are the eigenvalues of $\rho(g)$. Then χ is a generalized character of G.

Proof First suppose that we have proved this for one character θ. If θ' is another character of $\bar{\mathbb{F}}_q^\times$, then we claim that the same result is true for θ'. Indeed, let $\mathbb{F}_{q^m}$ be some field large enough to contain all the eigenvalues of the $\rho(g)$ with $g \in G$. The multiplicative group of $\mathbb{F}_{q^m}$ is cyclic, so $\theta'(t) = \theta(t^r)$ for all $t \in \mathbb{F}_q$, for some suitable r. Replacing S by the symmetric polynomial $S(X_1^r, \cdots, X_n^r)$, the truth of the theorem for θ' follows from the truth of the theorem for θ.

This means that we may choose the character θ at out convenience. We choose it to be the character θ used in our discussion of Brauer characters.

Next we note that it is enough to prove the theorem when

$$S(X_1, \cdots, X_n) = \sum_{i=1}^{n} X_i.$$

Indeed, if it is true for these polynomials, then applying the theorem to the exterior powers of the representation ρ, we obtain the truth of the theorem for the elementary symmetric polynomials, which generate the ring of all symmetric polynomials.

By Brauer's Theorem, it is sufficient to prove that $\chi(g) = \sum \theta(\alpha_i)$ is a generalized character when G is an elementary subgroup. We note that every elementary group can be written as $P \times Q$ where P is a p-group and Q has order prime to p. Indeed, if G is l-elementary, then writing $G = C \times L$ where C is cyclic of order prime to l and L is an l-group, if $l = p$ we may take $P = L$ and $Q = C$; and if $l \neq p$, we take P to be a p-Sylow subgroup of C, and Q to be the direct product of L with the remaining Sylow subgroups of C.

We show next that if $u \in P$ and $q \in Q$ then $\chi(uq) = \chi(q)$. Indeed, $\rho(u)$ and $\rho(q)$ commute, so after a change of basis we may assume that they are both upper triangular. Since $\rho(u)$ has p-power order, and since the characteristic of K is p, the upper-triangular matrix $\rho(p)$ is unipotent. Thus q and uq have the same eigenvalues, and the same value of χ.

Now the restriction of χ to Q is a Brauer character. Hence it is an ordinary character of Q by Theorem 5. As we have noted that χ factors through the projection $P \times Q \longrightarrow Q$, it is a character of $P \times Q$. $\square$