The calculation from last lecture showed that

$$\frac{1}{|G|}\sum_{g\in G}(R^{(k)}_{pm}g)(R^{(l)}_{nq}(g^{-1})) = \mu_k\delta_{nm}\delta_{pq}\delta_{kl} \tag{1}$$

where the $R^{(i)}$ are irreducible matrix representations of G, no two of which are equivalent. Note that k, l, m, n, p and q are free variables: the equation is valid for all their possible values. We can thus calculate the values of the scalars μ_k as follows. Put $l = k$ and $m = n$, and sum Eq. (1) over all values of n from 1 to d_k (the degree of $R^{(k)}$. After interchanging the order of summation on the left hand side we obtain

$$\frac{1}{|G|}\sum_{g\in G}\sum_{n=1}^{d_k}(R^{(k)}_{pn}g)(R^{(k)}_{nq}(g^{-1})) = \sum_{n=1}^{d_k}\mu_k\delta_{pq} = \mu_k d_k\delta_{pq}.$$

But since $(R^{(k)}g)(R^{(k)}(g^{-1})) = R^{(k)}(gg^{-1}) = R^{(k)}1 = I$ (for all values of g) we know that

$$\sum_{n=1}^{d_k}(R^{(k)}_{pn}g)(R^{(k)}_{nq}(g^{-1})) = I_{pq} = \delta_{pq},$$

and our equation above reduces to

$$\frac{1}{|G|}\sum_{g\in G}\delta_{pq} = \mu_k d_k\delta_{pq}.$$

So $\mu_k = d_k^{-1}$, and Eq. (1) becomes

$$\frac{1}{|G|}\sum_{g\in G}(R^{(k)}_{pm}g)(R^{(l)}_{nq}(g^{-1})) = d_k^{-1}\delta_{nm}\delta_{pq}\delta_{kl} \tag{2}$$

This basic result is known as the *orthogonality of coordinate functions*.

It was shown in Tutorial 1 that each matrix representation of a finite group is equivalent to a *unitary representation*, which by definition is a representation R such that Rg is a unitary matrix for each $g \in G$. (Recall that a matrix M is said to be unitary if its conjugate transpose is equal to its inverse; that is, $(\overline{M}^{\mathrm{t}})M = I$. In the case that the entries of M are real numbers this condition becomes $(M^{\mathrm{t}})M = I$, and the matrix is said to be orthogonal.) Let us review this proof before continuing.

Given a matrix representation $R\colon G \to \mathrm{GL}(d, \mathbb{C})$ we can make the complex vector space $V = \mathbb{C}^d$ (consisting of all d-component column vectors) into a left G-module by defining

$$gv = (Rg)v \qquad \text{(for all } g \in G \text{ and } v \in V).$$

The space V is of course an inner product space relative to the standard inner product, or dot product

$$\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_d\end{pmatrix}\cdot\begin{pmatrix}\mu_1\\ \mu_2\\ \vdots\\ \mu_d\end{pmatrix} = \overline{\lambda_1}\mu_1\overline{\lambda_2}\mu_2\cdots\overline{\lambda_d}\mu_d,$$

and as in our first proof of Maschke's Theorem we can obtain a G-invariant inner product on V by defining

$$v * u = \sum_{g \in G} (gv) \cdot (gu) \qquad \text{(for all } g \in G \text{ and } v,\, u \in V\text{)}.$$

Now choose a basis $v_1, v_2, \ldots, v_d$ of V which is orthonormal relative to this new inner product, and let S be the matrix representation of G which this new basis of V yields. That is,

$$gv_j = \sum_{i=1}^{d} (Sg)_{ij} v_i$$

for all $g \in G$ and $j \in \{1, 2, \ldots, d\}$. The representation S is then equivalent to the representation R; indeed, $Sg = T^{-1}(Rg)T$ (for all $g \in G$), where T is the transition matrix for changing coordinates relative to $v_1, v_2, \ldots, v_d$ into standard coordinates. Specifically, the j-th column of T is simply the column vector v_j. Furthermore, S is a unitary representation. To see this, note that G-invariance of $*$ yields (by definition) that $(gv) * (gu) = v * u$ for all $v,\, u \in V$, and now since the basis $v_1, v_2, \ldots, v_d$ is orthonormal

$$\begin{aligned}\delta_{jk} = v_j * v_k = (gv_j) * (gv_k) &= \Bigl(\sum_{i=1}^{d} (Sg)_{ij} v_i\Bigr) * \Bigl(\sum_{m=1}^{d} (Sg)_{mk} v_m\Bigr) = \sum_{i=1}^{d}\sum_{m=1}^{d} \overline{(Sg)_{ij}}(Sg)_{mk}(v_i * v_m)\\ &= \sum_{i=1}^{d}\sum_{m=1}^{d} \overline{(Sg)_{ij}}(Sg)_{mk}\delta_{im} = \sum_{i=1}^{d} \overline{(Sg)_{ij}}(Sg)_{ik} = \sum_{i=1}^{d} \bigl(\overline{Sg}^{\,\mathrm{t}}\bigr)_{ji}(Sg)_{ik}\end{aligned}$$

for all j and k and all $g \in G$. This shows that $\bigl(\overline{Sg}^{\,\mathrm{t}}\bigr)Sg = I$ for all $g \in G$, as required.

Returning to Eq. (2), let us now suppose that all the representations $R^{(i)}$ are unitary. Then for all $g \in G$ and all l,

$$R^{(l)}(g^{-1}) = (R^{(l)}g)^{-1} = \overline{R^{(l)}g}^{\,\mathrm{t}},$$

and so $R^{(l)}_{nq}(g^{-1}) = \overline{R^{(l)}_{qn}g}$. Hence Eq. (2) becomes

$$\frac{1}{|G|}\sum_{g \in G} (R^{(k)}_{pm}g)\bigl(\overline{R^{(l)}_{qn}g}\bigr) = d_k^{-1}\delta_{nm}\delta_{pq}\delta_{kl}. \tag{3}$$

Tabulating the values of the function $R^{(k)}_{pm}\colon G \to \mathbb{C}$ gives a row vector—let us temporarily call it x_{kpm}—which has one entry for each element of G. Equation (3) tells us that the standard dot product of x_{kpm} and x_{lqn} is zero unless k, p and m are (repectively) equal to l, q and n, in which case the dot product is $|G|/d_k$. For each value of k there are d_k^2 possibilities for the ordered pair (p, m) (since $p,\, m \in \{1, 2, \ldots, d_k\}$), and so we have $\sum_{k=1}^{s} d_k^2$ vectors x_{kpm} altogether. These vectors are linearly independent since they are nonzero and pairwise orthogonal, and so they span a space of dimension $\sum_{k=1}^{s} d_k^2$. As they are contained in the $|G|$-dimensional space of row vectors with $|G|$ components, we conclude that

$$\sum_{k=1}^{s} d_k^2 \le |G| \tag{4}$$

whenever G has mutually inequivalent representations of degrees $d_1, d_2, \ldots, d_s$. Thus $s \le |G|$, since each d_k is at least 1, and this shows that no group G can have more than $|G|$ mutually inequivalent irreducible representations. In particular, up to equivalence the number of irreducible complex representations of a finite group is finite. (In fact, as we shall show in a few lectures' time, equality always holds in (4).)

Let us illustrate the above result for the group $G = S_3$. We know three irreducible mutually inequivalent representations, of degrees 1, 1 and 2. The sum of the squares of these degrees is 6, which equals the order of S_3; so, in view of the inequality (4), there can be no fourth irreducible representation which is not equivalent to one of the these three. Representations of degree 1 are necessarily unitary (for a finite group), since on the one hand the representation has to be equivalent to a unitary representation (see above), and on the other hand a representation of degree 1 cannot be equivalent to anything but itself since 1×1 matrices commute. If we identify S_3 with the group of symmetries of an equilateral triangle, and coordinatize the Euclidean plane by taking the centroid of the triangle as the origin and the line through the origin and one of the vertices as the x-axis, then we obtain a representation of S_3 by real orthogonal matrices. It is now a straightforward matter to compute the values of the coordinate functions of our three irreducible representations, and obtain the following table.

g	id	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$R^{(1)}_{11}g$	1	1	1	1	1	1
$R^{(2)}_{11}g$	1	-1	-1	-1	1	1
$R^{(3)}_{11}g$	1	$-1/2$	$-1/2$	1	$-1/2$	$-1/2$
$R^{(3)}_{12}g$	0	$\sqrt{3}/2$	$-\sqrt{3}/2$	0	$-\sqrt{3}/2$	$\sqrt{3}/2$
$R^{(3)}_{21}g$	0	$\sqrt{3}/2$	$-\sqrt{3}/2$	0	$\sqrt{3}/2$	$-\sqrt{3}/2$
$R^{(3)}_{22}g$	1	$1/2$	$1/2$	-1	$-1/2$	$-1/2$

Here, for example, the last four entries of the second column say that the matrix $R^{(3)}(1,2)$ is $\begin{pmatrix} -1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$, which is the matrix of the reflection in the line through the origin with slope $\tan(\pi/3)$. (The vertices 1, 2 and 3 of the triangle are, respectively, the points with coordinates $\begin{pmatrix} x \\ y \end{pmatrix}$ given by $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} -1/2 \\ \sqrt{3}/2 \end{pmatrix}$ and $\begin{pmatrix} -1/2 \\ -\sqrt{3}/2 \end{pmatrix}$ respectively.

Interpreting the values in the table above as the entries of a 6×6 matrix, we can check easily that the dot product of two distinct rows of the matrix is 0, while the dot product of a row with itself is six (for the first two rows) or three (for the last four rows). In general, Eq. (2) says that the table of values of the coordinate functions is a matrix whose rows are mutually orthogonal, the length of each row being given by $\sqrt{d/|G|}$, where d is is the degree of the relevant representation. Dvividing each row by its length yields a matrix $T(G)$ whose rows form an orthonormal set of vectors; the rows of $T(G)$ are indexed by triples $\{\,(k,p,m) \mid 1 \le k \le s \text{ and } p,\, m \in \{1,2,\ldots,d_k\}\,\}$ and the columns by elements of G, the $((k,p,m),g)$-entry being $\sqrt{d/|G|}R^{(k)}_{p,m}g$. For S_3 we find that

$$T(S_3) = \begin{pmatrix} 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} \\ 1/\sqrt{6} & -1/\sqrt{6} & -1/\sqrt{6} & -1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} \\ 1/\sqrt{3} & -1/2\sqrt{3} & -1/2\sqrt{3} & 1/\sqrt{3} & -1/2\sqrt{3} & -1/2\sqrt{3} \\ 0 & 1/2 & -1/2 & 0 & -1/2 & 1/2 \\ 0 & 1/2 & -1/2 & 0 & 1/2 & -1/2 \\ 1/\sqrt{3} & 1/2\sqrt{3} & 1/2\sqrt{3} & -1/\sqrt{3} & -1/2\sqrt{3} & -1/2\sqrt{3} \end{pmatrix},$$

which is unitary—orthogonal, in fact, since it is real—as one can easily check.

A square matrix M is unitary if and only if its columns form an orthonormal set of vectors, since this condition is clearly equivalent to the matrix equation $(\overline{M}^{\,\mathrm{t}})M = I$. Since this in turn is equivalent to $M(\overline{M}^{\,\mathrm{t}}) = I$, which says that the rows form an orthonormal set, we conclude that the rows of a square matrix are orthonormal if and only if the columns are too. Given that equality holds in (4), so that $T(G)$ is square, column orthogonality tells us that for all g, $h \in G$

$$\frac{1}{|G|}\sum_{k,p,m} d_k\,\overline{\big(R^{(k)}_{pm}g\big)}\,\big(R^{(k)}_{pm}h\big) = \delta_{gh}.$$

(This is equivalent to Eq. (2), but much less important in practice.)

Lecture 10, 27/8/97

The regular representation

If a group G has a left action on a set S then associated with each $g \in G$ is a permutation $\sigma_g\colon S \to S$ defined by $\sigma_g s = gs$ for all $s \in S$. Furthermore, $g \mapsto \sigma_g$ is a homomorphism from G to the group of all permutations of S. We have also seen that permutations can be associated with permutation matrices. If $S = \{s_1, s_2, \ldots, s_d\}$ we thus obtain a homomorphism $g \mapsto Rg$ from G to the group of all $d \times d$ permutation matrices, where the (i, j)-entry of Rg is 1 if $v_i = gv_j$ and 0 otherwise.* In other words, a permutation representation becomes a matrix representation if one identifies permutations with permutation matrices. (The G-module associated with this matrix representation is a vector space with basis in bijective correspondence with the elements of S, the elements of G acting via linear transformations which permute this basis.)

If we consider in particular the left multiplication action of the group G on itself then we obtain a representation of G by $|G| \times |G|$ permutation matrices. The precise matrices depend on a chosen ordering of the elements of G. Let us illustrate what happens for the group S_3, using the same ordering of the elements as we used in the multiplication table given in Lecture 1:

$$g_1 = \mathrm{id},\ g_2 = (1\,2\,3),\ g_3 = (1\,3\,2),\ g_4 = (1\,2),\ g_5 = (1\,3),\ g_6 = (2\,3).$$

Left multiplication by $(1\,2)$ swaps g_1 and g_4 (since $(1\,2)\mathrm{id} = (1\,2)$ and $(1\,2)(1\,2) = \mathrm{id}$), and also swaps the pairs g_2, g_6 and g_3, g_5. The matrix representing $(1\,2)$ thus comes out to be

$$R(1\,2) = \begin{pmatrix} 0&0&0&1&0&0\\ 0&0&0&0&0&1\\ 0&0&0&0&1&0\\ 1&0&0&0&0&0\\ 0&0&1&0&0&0\\ 0&1&0&0&0&0 \end{pmatrix}.$$

Similarly

$$R(2\,3) = \begin{pmatrix} 0&0&0&0&0&1\\ 0&0&0&0&1&0\\ 0&0&0&1&0&0\\ 0&0&1&0&0&0\\ 0&1&0&0&0&0\\ 1&0&0&0&0&0 \end{pmatrix}, \qquad R(1,\,2,\,3) = \begin{pmatrix} 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0 \end{pmatrix}.$$

* In the case of a right action of G on S the permutation matrix associated with $g \in G$ should have (i, j)-entry 1 if $v_i g = v_j$ and 0 otherwise, to ensure that $R(gh)$ equals $(Rg)(Rh)$ rather than $(Rh)(Rg)$.

The others are equally easy to calculate.

The representation $R\colon G \to \mathrm{GL}(|G|, \mathbb{C})$ constructed in this way is called the *regular representation* of G. In view of Maschke's Theorem it is possible to find a matrix T—rather, I should say *there exists* a matrix T, since it not clear how to find one—such that

$$T^{-1}(Rg)T = \begin{pmatrix} S_1g & 0 & 0 & \cdots & 0 \\ 0 & S_2g & 0 & \cdots & 0 \\ 0 & 0 & S_3g & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & S_mg \end{pmatrix} \tag{1}$$

where S_1, S_2, $\ldots$, S_m are some irreducible representations of G. Note that the order in which the irreducibles S_i occur as diagonal summands can be varied by altering the matrix T. For example, S_1 and S_2 can be interchanged since

$$\begin{pmatrix} 0 & I & \cdots & 0 \\ I & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} \begin{pmatrix} S_1g & 0 & \cdots & 0 \\ 0 & S_2g & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & S_mg \end{pmatrix} \begin{pmatrix} 0 & I & \cdots & 0 \\ I & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} = \begin{pmatrix} S_2g & 0 & \cdots & 0 \\ 0 & S_1g & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & S_mg \end{pmatrix}$$

and clearly a sequence of similar such operations can produce any desired ordering of the diagonal summands. Furthermore, each S_i can be replaced by any representation to which it is equivalent: for example, if $S_1'g = X^{-1}(S_1g)X$ then

$$\begin{pmatrix} X & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix}^{-1} \begin{pmatrix} S_1g & 0 & \cdots & 0 \\ 0 & S_2g & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & S_mg \end{pmatrix} \begin{pmatrix} X & 0 & \cdots & 0 \\ 0 & I & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & I \end{pmatrix} = \begin{pmatrix} S_1'g & 0 & \cdots & 0 \\ 0 & S_2g & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & S_mg \end{pmatrix}$$

for all $g \in G$. So if we choose irreducible representations $R^{(1)}$, $R^{(2)}$, $\ldots$, $R^{(s)}$ such that every irreducible representation of G is equivalent to one of the $R^{(k)}$, then we may assume that each S_j in Eq. (1) above coincides with some $R^{(k)}$. Of course, a given $R^{(k)}$ could conceivably occur several times. So that we can apply the formulas from Lecture 9, we shall assume that the $R^{(k)}$ are unitary and mutually inequivalent. As we shall soon see, it turns out that each $R^{(k)}$ occurs d_k times as a diagonal summand in Eq. (1). This means that the degree of the representation on the right hand side in Eq.(1) is $\sum_k d_k^2$ (since for each k there are d_k summands of degree d_k). As has already been mentioned, this equals $|G|$, which is the degree of the representation on the left hand side of Eq. (1).

The coordinate space of a representation

In this course $\mathbb{C}^n$ usually means the vector space of n-component column vectors over $\mathbb{C}$. Other authors often define it to be the space of row vectors. A third alternative would be to identify $\mathbb{C}^n$ with the space of all complex valued functions on the set $\{1, 2, \ldots, n\}$. Indeed, a function $f\colon \{1, 2, \ldots, n\} \to \mathbb{C}$ is nothing other than an n-tuple of values: f can be identified with the n-component vector whose ith component is fi. The moral of this story is simply that the set of all complex valued functions on an n-element set S is a vector space of dimension n. Addition and scalar multiplication are defined by the formulas $(f + g)s = (fs) + (gs)$ and $(\lambda f)s = \lambda(fs)$.

Let V_G be the $|G|$-dimensional space of all complex valued functions on G. The *coordinate space* of a matrix representation $S\colon G \to \mathrm{GL}(d, \mathbb{C})$ is the subspace of V_G which is spanned by the coordinate functions of S. That is, for all i, $j \in \{1, 2, \ldots, d\}$ define $S_{ij}: G \to \mathbb{C}$, so that $S_{ij}g$ is the (i, j) entry of Sg; the coordinate space is then the space spanned by all the functions S_{ij}.

Proposition. *Equivalent representations have the same coordinate space.*

Proof. Let R and S be equivalent matrix representations of G ofdegree d, so that there exists an invertible $d \times d$ matrix T such that $T^{-1}(Rg)T = Sg$ for all $g \in G$. Let R_{ij} and S_{ij} be the coordinate functions of R and S, and denote the (i, j) entries of T and T^{-1} by T_{ij} and U_{ij} respectively. Then for all $g \in G$ we have that

$$S_{ij}g = \sum_{k=1}^{d}\sum_{l=1}^{d} U_{ik}(R_{kl}g)T_{lj}$$

whence it follows that

$$S_{ij} = \sum_{k,l}(U_{ik}T_{lj})R_{kl}$$

for all i, $j \in \{1, 2, \ldots, d\}$. Since this expresses each coordinate function of S as a linear combination of the coordinate functions of R, it follows that the coordinate functions of S are all contained in the coordinate space of R, and hence the coordinate space of S is contained in the coordinate space of R. But equivalence of representations is a symmetric relation, and so the same argument shows that the coordinate space of R is contained in that of S. □

Note also the following result, which is fairly trivial.

Proposition. *The coordinate space of the diagonal sum of two representations R and S is the vector space sum of the coordinate spaces of R and S.*

Proof. Let m be the degree of R and n the degree of S, and let T be the diagonal sum, given by

$$Tg = \begin{pmatrix} Rg & 0 \\ 0 & Sg \end{pmatrix}$$

for all $g \in G$. Denote the coordinate functions of R by R_{ij}, and denote those of S and T similarly. For i, $j \in \{1, 2, \ldots, m\}$ we see that $T_{ij} = R_{ij}$, while for i, $j \in \{m+1, m+2, \ldots, m+n\}$ we have $T_{ij} = S_{i-m,j-m}$. Furthermore, all other coordinate functions of T are zero. So an arbitrary element $\sum_{i,j} \lambda_{ij}T_{ij}$ of the coordinate space of T can be expressed as

$$\sum_{i\leq m,\, j\leq m} \lambda_{ij}R_{ij} + \sum_{i>m,\, j>m} \lambda_{ij}S_{i-m,j-m},$$

which is in the sum of the coordinate spaces of R and S. □

By Maschke's Theorem we know that every complex representation of a finite group is equivalent to a diagonal sum of irreducible representations. So if, as above, we fix a full set of irreducible representations* $R^{(1)}$, $R^{(2)}$, ..., $R^{(s)}$ then the coordinate space of an arbitrary representation is contained in the sum of the coordinate spaces of the $R^{(k)}$. We shall now prove a result which, though easy, is crucial for our cause.

Proposition. *The coordinate space of the regular representation equals V_G, the space of all complex valued functions on G.*

* That is, one from each equivalence class of irreducibles

Proof. The coordinate space of the regular representation is of course contained in V_G; so we have only to prove the reverse inclusion.

Let g_1, g_2, …, g_n be the elements of G, so that in particular the degree of the regular representation is n, and let $g \in G$ be arbitrary. We can choose i, $j \in \{1, 2, \dots, n\}$ such that $g_i = gg_j$: for example, choose j so that g_j is the identity element and i so that $g_i = g$. Now the coordinate function R_{ij} of the regular representation R satisfies, for all $h \in G$,

$$\begin{aligned} R_{ij}h &= \begin{cases} 1 & \text{if } g_i = hg_j \\ 0 & \text{otherwise,} \end{cases} \\ &= \begin{cases} 1 & \text{if } h = g \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

The function R_{ij} is thus the analogue of a row vector which has one component equal to 1 and all other components 0. Furthermore, the positioning of the 1 corresponds to the choice of the element h, which was arbitrary. The set of all functions of this form spans V_G. Explicitly, if $f\colon G \to \mathbb{C}$ is arbitrary then

$$f = \sum_{i=1}^{n} (fi) R_{ij}$$

where j is fixed so that g_j is the identity element. □

The coordinate space of the irreducible representation $R^{(k)}$ is spanned by the d_k^2 coordinate functions $R^{(k)}_{pm}$ (where p, $m \in \{1, 2, \dots, d_k\}$), and the sum of the coordinate spaces of $R^{(1)}$, $R^{(2)}$, …, $R^{(s)}$ is spanned by the totality of all coordinate functions $R^{(k)}_{pm}$ for (k, p, m) in the set $\mathcal{S} = \{\, (k, p, m) \mid 1 \le k \le s \text{ and } p,\ m \in \{1, 2, \dots, d_k\} \,\}$. But this sum of coordinate spaces must equal the full space V_G of complex valued functions on G, since it must contain the coordinate space of the regular representation, and so the number of elements in the spanning set $\mathcal{S}$ must be at least $|G| = \dim V_G$. So we conclude that $\sum_{k=1}^{s} d_k^2 \ge |G|$, and hence $\sum_{k=1}^{s} d_k^2 = |G|$ since the reverse inequality was obtained previously. Since this also shows that the number of elements in $\mathcal{S}$ equals the dimension of V_G, which it spans, it follows that the elements of $\mathcal{S}$ are linearly independent.