As several people pointed out after last lecture, my description of the representation of the quaternion group as a subgroup of $\mathrm{GL}(2,3)$ was incorrect. The matrices A_1, A_2 and A_3 should be as follows:

$$A_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Representations, linear actions and modules.

Recall that if V is a vector space over the field F and G is a group, then an action of G on V is a function $(g,v) \mapsto gv$ from $G \times V$ to V such that
(i) $(gh)v = g(hv)$ for all g, $h \in G$ and $v \in V$,
(ii) $1v = v$ for all $v \in V$, where 1 is the identity element of G,
(iii) $g(u+v) = gu + gv$ for all $g \in G$ and u, $v \in V$,
(iv) $g(\lambda v) = \lambda(gv)$ for all $g \in G$ and $v \in V$, and all $\lambda \in F$.
(Note that, by our definitions, an action of G on the vector space V is not the same thing as an action of G on the set V: items (iii) and (iv) are not required for the latter. This terminology can lead to confusion, and it would perhaps be better to always refer to an action of G on V that satisfies (iii) and (iv) as a *linear* action. However, in this course the only group actions we will encounter on sets which are vector spaces will be linear actions.) We have already noted that an action of a group G on a set S is essentially the same as a permutation representation of G on S. In the same way, a linear action of a group G on a vector space V is essentially the same as a representation of G by linear transformations on V.

Proposition. *Given an action of a group G on a vector space V, for each $g \in G$ define a function $\rho g\colon V \to V$ by $(\rho g)v = gv$ for all $v \in V$. Then ρg is an invertible linear transformation, and the function ρ defined by $g \mapsto \rho g$ is a homomorphism from G to the group of all invertible linear transformations on V. Conversely, given a homomorphism ρ from G to the group of invertible linear transformations on V, the formula $gv = (\rho g)v$ defines an action of G on V.*

Proof. Suppose first that the action is given. Since we have an action of G on the set V we know from the earlier argument that $g \mapsto \rho g$ is a homomorphism from G to the group of all invertible functions $V \to V$, and so all we have to show is that each function ρg is also linear. But this is precisely what items (iii) and (iv) above say:

$$\begin{aligned}(\rho g)(v+w) &= g(v+w) = gv + gw = (\rho g)v + (\rho g)w\\ (\rho g)(\lambda v) &= g(\lambda v) = \lambda(gv) = \lambda((\rho g)v)\end{aligned}$$

for all v, $w \in V$ and $\lambda \in F$.

Conversely, suppose that the homomorphism ρ is given. If we ignore the fact that the functions ρg are linear, and focus instead on the fact that they are bijective functions $V \to V$, then $g \mapsto \rho g$ can be regarded as a permutation representation of G on the set V, and hence it follows that $gv = (\rho g)v$ defines an action of G on the set V. So we just have to show that the action is linear; that is, that (iii) and (iv) are satisfied. Of course, this is exactly what the linearity of ρg tells us:

$$\begin{aligned}g(v+w) &= (\rho g)(v+w) = (\rho g)v + (\rho g)w = gv + gw\\ g(\lambda v) &= (\rho g)(\lambda v) = \lambda((\rho g)v) = \lambda(gv)\end{aligned}$$

for all v, $w \in V$ and $\lambda \in F$.

So a representation of a group on a vector is the same thing as an action of a group on a vector space. Well then, why not introduce a third term to describe this same situation!

Definition. A vector space V on which a group G has an action is called a G-module.

Very naturally, we should investigate functions from G-modules to G-modules which preserve the G-module structure, as well as investigating circumstances in which a subset of a G-module is also a G-module. Hence we make the following definitions:

Definition. (i) A submodule of a G-module V is a vector subspace U of V such that $gu \in U$ for all $g \in G$ and $u \in U$.
(ii) If U and V are G-modules then a G-homomorphism from U to V is a linear transformation $f\colon U \to V$ such that $f(gu) = g(fu)$ for all $g \in G$ and $u \in U$.

We shall have much more to say about G-modules. In particular, there is a G-module version of the First Isomorphism Theorem, which will be of great importance for the theory we shall develop. Also important is the concept of the direct sum of two G-modules, analogous to direct sums in group theory and vector space theory. However, before pursuing such matters, there is another basic aspect of representations that ought to be noted.

Representations and matrix representations

Let U, V be finite-dimensional vector spaces over the field F, of dimensions m and n respectively, and let $f\colon U \to V$ be a linear map. If $\mathcal{B}$ is a basis of U and $\mathcal{C}$ a basis of V then the matrix of f relative to $\mathcal{B}$ and $\mathcal{C}$ is the $n \times m$ matrix $M_{\mathcal{C}\,\mathcal{B}}(f)$ whose (i, j)-entry is the scalar a_{ij}, where

$$fu_j = \sum_{i=1}^{n} a_{ij} v_i \qquad \text{for all } j = 1, 2, \ldots, m,$$

$u_1, u_2, \ldots, u_m$ being the vectors that comprise the basis $\mathcal{B}$, and $v_1, v_2, \ldots, v_n$ those that comprise the basis $\mathcal{C}$. The fundamentals of the connection between matrices and linear transformations should be familiar to you from 2nd year work. The principal facts are as follows. Multiplying the coordinate vector relative to $\mathcal{B}$ of an element $u \in U$ by $M_{\mathcal{C}\,\mathcal{B}}(f)$ yields the coordinate vector relative to $\mathcal{C}$ of $fu \in V$; that is, if $u = \sum_{j=1}^{m} \lambda_j u_j$ then $fu = \sum_{i=1}^{n} \lambda_i v_i$, where

$$M_{\mathcal{C}\,\mathcal{B}}(f) \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_m \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

If the bases $\mathcal{B}$ and $\mathcal{C}$ are fixed, the mapping $f \mapsto M_{\mathcal{C}\,\mathcal{B}}(f)$ is a bijective correspondence between the set of all linear maps $U \to V$ and the set of all $n \times m$ matrices over F. If $f\colon U \to V$ and $h\colon V \to W$ are both linear maps, and $\mathcal{D}$ is a basis of the vector space W, then $M_{\mathcal{D}\,\mathcal{B}}(hf) = M_{\mathcal{D}\,\mathcal{C}}(h) M_{\mathcal{C}\,\mathcal{B}}(f)$. And similarly, if h and f are two linear maps from U to V then $M_{\mathcal{C}\,\mathcal{B}}(h + f) = M_{\mathcal{C}\,\mathcal{B}}(h) + M_{\mathcal{C}\,\mathcal{B}}(f)$. In particular we have that

$$\begin{aligned} M_{\mathcal{C}\,\mathcal{C}}(hf) &= M_{\mathcal{C}\,\mathcal{C}}(h) M_{\mathcal{C}\,\mathcal{C}}(f) \\ M_{\mathcal{C}\,\mathcal{C}}(h + f) &= M_{\mathcal{C}\,\mathcal{C}}(h) + M_{\mathcal{C}\,\mathcal{C}}(f) \end{aligned}$$

for all linear transformations h, $f : V \to V$. Since the matrix of the identity linear transformation is the identity matrix, it follows from the first of these two equations that a linear transformation

$V \to V$ is invertible if and only if its matrix relative to $\mathcal{C}$ is invertible, and we deduce that $f \mapsto M_{\mathcal{C}\,\mathcal{C}}(f)$ is an isomorphism from the group of all invertible linear transformations on V to the group of all invertible $n \times n$ matrices over F.

Definition. The group of all invertible linear transformations on a vector space V is called the *general linear group* $\mathrm{GL}(V)$ of the space V. The group of invertible $d \times d$ matrices over F is written as $\mathrm{GL}(d, F)$, and is called the general linear group of degree d over F.

We have defined a (linear) representation of G on V to be a homomorphism $\rho: G \to \mathrm{GL}(V)$. Similarly, a *matrix representation* of G is a homomorphism $G \to \mathrm{GL}(d, F)$; the integer d is called the degree of the representation. If ρ is a representation of G on a d-dimensional vector space V, and if $\mathcal{C}$ is a basis of V, then we obtain a matrix representation of G of degree d by defining $Rg = M_{\mathcal{C}\,\mathcal{C}}(\rho g)$ for each $g \in G$. The map $R: G \to \mathrm{GL}(d, F)$ is certainly a homomorphism since it is the composite of the homomorphism $g \mapsto \rho g$ from G to $\mathrm{GL}(V)$ and the isomorphism $f \mapsto M_{\mathcal{C}\,\mathcal{C}}(f)$ from $\mathrm{GL}(V)$ to $\mathrm{GL}(d, F)$. Hence R is a matrix representation, as claimed. Conversely, given a matrix representation $R: G \to \mathrm{GL}(d, F)$ we can obtain a representation $\rho: G \to \mathrm{GL}(V)$ by defining ρg to be the linear transformation whose matrix relative to $\mathcal{C}$ is Rg. The moral of this story is this: once a basis of V is fixed, a representation of G on V is essentially the same thing as a matrix representation of G of degree $d = \dim V$.

Since the choice of a basis for a vector space is a somewhat arbitrary matter, it is natural to investigate the relationship between two matrix representations that are derived from the same representation $\rho: G \to \mathrm{GL}(V)$ by choosing two different bases. So suppose that $\mathcal{B}$ and $\mathcal{C}$ are bases of V, and let $R,\ S : G \to \mathrm{GL}(d, F)$ be defined by the formulas $Rg = M_{\mathcal{C}\,\mathcal{C}}(\rho g)$ and $Sg = M_{\mathcal{B}\,\mathcal{B}}(\rho g)$, for all $g \in G$. If $T = M_{\mathcal{B}\,\mathcal{C}}(\mathrm{id})$ then we find that for all $g \in G$,

$$T(Rg) = M_{\mathcal{B}\,\mathcal{C}}(\mathrm{id})M_{\mathcal{C}\,\mathcal{C}}(\rho g) = M_{\mathcal{B}\,\mathcal{C}}((\mathrm{id})(\rho g)) = M_{\mathcal{B}\,\mathcal{C}}((\rho g)(\mathrm{id})) = M_{\mathcal{B}\,\mathcal{B}}(\rho g)M_{\mathcal{B}\,\mathcal{C}}(\mathrm{id}) = (Sg)T.$$

Since $M_{\mathcal{B}\,\mathcal{C}}(\mathrm{id})M_{\mathcal{C}\,\mathcal{B}}(\mathrm{id}) = M_{\mathcal{B}\,\mathcal{B}}(\mathrm{id}) = I$, and similarly $M_{\mathcal{C}\,\mathcal{B}}(\mathrm{id})M_{\mathcal{B}\,\mathcal{C}}(\mathrm{id}) = M_{\mathcal{C}\,\mathcal{C}}(\mathrm{id}) = I$, we see that the matrix T is invertible. Hence $Sg = T(Rg)T^{-1}$ for all $g \in G$.

Definition. Matrix representations $R,\ S : G \to \mathrm{GL}(d, F)$ are said to be *equivalent* if there exists $T \in \mathrm{GL}(d, F)$ such that $Sg = T(Rg)T^{-1}$ for all $g \in G$.

Lecture 4, 6/8/97

Some representations of the symmetric group of degree 3

Let σ be a permutation of $\{1, 2, \ldots, n\}$. If V is a vector space (over any field F) with basis $v_1, v_2, \ldots, v_n$ then there is a linear transformation $p_\sigma: V \to V$ such that $v_i \mapsto v_{\sigma j}$ for each j. That is, $p_\sigma v_j = \sum_{i=1}^{n} \delta_{i\,\sigma j} v_i$. Thus the matrix of p_σ relative to the basis $v_1, v_2, \ldots, v_n$ is the matrix P_σ whose (i, j)-entry is $\delta_{i\,\sigma j}$. We call P_σ the *permutation matrix* corresponding to σ. It is trivial to check from the definition that if σ and τ are permutations of $\{1, 2, \ldots, n\}$ then $p_{\sigma\tau} = p_\sigma p_\tau$: indeed, for all j we have

$$p_{\sigma\tau} v_j = v_{(\sigma\tau)j} = v_{\sigma(\tau j)} = p_\sigma(v_{\tau j}) = p_\sigma(p_\tau v_j) = (p_\sigma p_\tau)v_j,$$

and as the linear maps $p_{\sigma\tau}$ and $p_\sigma p_\tau$ have the same effect on all elements of the basis $v_1, v_2, \ldots, v_n$ it follows that they are equal. Note also that if id is the identity permutation then p_{id} is the identity transformation of V. Thus it follows that p_σ is invertible for all $\sigma \in S_n$, and $p: S_n \to \mathrm{GL}(V)$ defined by $p\sigma = p_\sigma$ is a representation of S_n. By the general theory we have described, any choice of a basis of V gives rise to a matrix representation $S_n \to \mathrm{GL}(n, F)$ corresponding to the representation p. Of course, if we make the obvious choice and use the basis $v_1, v_2, \ldots, v_n$, the matrix representation we obtain is given by $\sigma \mapsto P_\sigma$.

When written out explicitly in the case $n = 3$, the matrix representation we have described above is as follows:

$$\begin{array}{lll}
\mathrm{id} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & (1,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} & (1,2,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\
(1,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} & (2,3) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & (1,3,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}
\end{array}$$

Since $\det(AB) = \det A \det B$ whenever A and B are $d \times d$ matrices, we see that if $R\colon g \mapsto Rg$ is a matrix representation of degree d of any group G, then $g \mapsto \det(Rg)$ is a matrix representation of degree 1 of the group G. Applying this observation to the above representation of S_3 yields the representation given by

$$\begin{array}{lll}
\mathrm{id} \mapsto 1 & (1,3) \mapsto -1 & (1,2,3) \mapsto 1 \\
(1,2) \mapsto -1 & (2,3) \mapsto -1 & (1,3,2) \mapsto 1.
\end{array}$$

This representation can alternatively be described by the rule that even permutations are mapped to 1 and odd permutations to -1. There is another even more obvious representation of S_3 of degree 1: it is given by $\sigma \mapsto 1$ for all $\sigma \in S_3$. (Of course this works in the same way for any group G at all. The representation given by $g \mapsto 1$ for all g is called the 1-representation, or the principal representation, of G).

Making use of the terminology introduced in Lecture 3 we may call the three dimensional space V with basis v_1, v_2, v_3 an S_3-module. The S_3-action is given by $\sigma v_j = v_{\sigma j}$ for all $\sigma \in S_3$ and all $j \in \{1, 2, 3\}$. It is fairly easy to see that the subset U of V defined by

$$U = \{\, \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 \mid \lambda_1 + \lambda_2 + \lambda_3 = 0 \,\}$$

is an S_3-submodule of V. To prove this it suffices to show that U is closed under addition and scalar multiplication, and also closed under the action of elements of S_3. This is left as an exercise for the student. The student can also check that $u_1 = v_1 - v_2$ and $u_2 = v_2 - v_3$ form a basis for U, and the matrices relative to this basis of the transformations of U corresponding to the various elements of S_3 are as follows:

$$\begin{array}{lll}
\mathrm{id} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & (1,3) \mapsto \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} & (1,2,3) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \\
(1,2) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} & (2,3) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} & (1,3,2) \mapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.
\end{array}$$

Thus we have obtained a matrix representation of S_3 of degree 2.

Let us assume, for definiteness, that the field F (the scalar field for V and the coefficient field for our matrices) is $\mathbb{C}$, the field of complex numbers. The two representations of S_3 of degree 1 and the representation of S_3 of degree 2 that we have described above are all irreducible representations of S_3, in a sense that we will define shortly. Moreover, it turns out that any irreducible complex representation of S_3 has to be equivalent to one of these three. The major theorems of representation theory that we will discuss in this course tell us in principle how an arbitrary complex representation of a finite group G can be expressed in terms of irreducible complex representations, and how many equivalence classes of irreducible complex representations a finite group has. There is no known uniform method of constructing the irreducible representations of an arbitrary finite group, and consequently the main practical problem of representation theory is to find elegant descriptions of the irreducible representations of various important classes of finite groups. In truth, there are not very many classes of groups for which this goal has been achieved, but the symmetric groups constitute a class for which a complete theory has been discovered. It is hoped that some of this theory will be described before the end of this course.

Centralizers and conjugacy

Proposition. *Let G be a group and $g \in G$. Then the set $C_G(g) = \{ x \in G \mid xg = gx \}$ is a subgroup of G.*

Proof. We must show that $1 \in C_G(g)$, that $x^{-1} \in C_G(g)$ whenever $x \in C_G(g)$, and that $xy \in C_G(g)$ whenever $x, y \in C_G(g)$. All of these are trivial. Since the defining property of the identity element is that $1g$ and $g1$ both equal g, we have $1g = g1$, and hence $1 \in C_G(g)$. If $x \in C_G(g)$ then $xg = gx$, and multiplying this equation on the left and on the right by x^{-1} gives $gx^{-1} = x^{-1}g$, whence $x^{-1} \in C_G(g)$. And if $x, y \in C_G(g)$ then $xg = gx$ and $yg = gy$, and we see that

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy),$$

whence $xy \in C_G(g)$, as required. □

Definition. The subgroup $C_G(g)$ defined in the above proposition is called the *centralizer* in G of the element g.

Recall that if H is a subgroup of a group G then for each $x \in G$ the subset $xH = \{ xh \mid h \in H \}$ is called a *left coset* of H in G. The mapping $h \mapsto xh$ from H to xH is a bijection, and so the number of elements of the coset xH is the same as the number of elements of G. If $x, y \in G$ then the left cosets xH and yH either coincide or are disjoint. They coincide if $x \in yH$, or (equivalently) if $y \in xH$, or (a third equivalent condition) if $x^{-1}y \in H$. Furthermore, every element of G lies in some left coset of H: indeed, $g \in gH$. It follows that we may choose a *left transversal*, or *system of representatives of the left cosets*, for the subgroup H. This is a family $(x_i)_{i \in I}$ of elements of G such that G is the disjoint union of the cosets x_iH for $i \in I$. Assuming that the group G is finite then of course the number of left cosets of H is finite too. The number of left cosets of H in G is called the *index* of H in G, denoted by $[G : H]$. If $n = [G : H]$ then a left transversal for H will consist of n elements $x_1, x_2, \ldots, x_n$, and since

$$G = x_1H \cup x_2H \cup \cdots \cup x_nH$$

expresses G as the disjoint union of $n = [G : H]$ sets all of which have $|H|$ elements, we conclude that $|G| = [G : H]|H|$.

Suppose now that $H = C_G(g)$, where $g \in G$. If $x, y \in G$ are in the same left coset of H, then $y = xh$ for some $h \in H$, and

$$ygy^{-1} = (xh)g(xh)^{-1} = x(hg)h^{-}x^{-1} = x(gh)h^{-1}x^{-1} = xgx^{-1},$$

since h is in the centralizer of g. Thus we have shown that $ygy^{-1} = xgx^{-1}$ whenever x, y are in the same left coset of the centralizer. Conversely, if $ygy^{-1} = xgx^{-1}$ then $(x^{-1}y)g = g(x^{-1}y)$, so that $x^{-1}y \in C_G(g)$, and hence x and y are in the same coset of the centralizer. Thus the elements of G of the form xgx^{-1} are in one to one correspondence with the left cosets of $C_G(g)$: if $x_1, x_2, \ldots, x_n$ is a left transversal then every element of the form xgx^{-1} equals one or other of the n elements $x_igx_i^{-1}$, and these elements are all distinct (since they correspond to distinct cosets). These elements of the form xgx^{-1} are called the *conjugates* of g in G; we have shown that the number of conjugates of G equals the index of the centralizer of g.