The First Isomorphism Theorem *Let V and W be G-modules and let $f: V \to W$ be a G-homomorphism. Then*

$$\ker f = \{ v \in V \mid fv = 0 \}$$

is a G-submodule of V,

$$\operatorname{im} f = \{ fv \mid v \in V \}$$

is a G-submodule of W, and there is a G-isomorphism $V/\ker f \to \operatorname{im} f$ such that $v + U \mapsto gv$ for all $v \in V$.

A similar theorem is valid for vector spaces without any G-actions: if U and V are vector spaces an $f: V \to W$ a linear map then the kernel and image of f are subspaces of V and W, and the quotient space $V/\ker f$ is isomorphic to $\operatorname{im} f$. This result is sometimes called "The Main Theorem on Linear Mappings". Because two vector spaces are isomorphic if and only if they have the same dimension, it is common to state the result in terms of dimensions, and since it is easily shown that $\dim(V/U) = \dim V - \dim U$ the statement becomes $\dim V = \dim(\ker f) + \dim(\operatorname{im} f)$.

Turning to the proof of the theorem in the form stated above, let us first show that $\ker f$ is a G-submodule of V. Since f is linear we have that $f(0_V) = 0_W$, and so $0_V \in \ker f$. If v_1, $v_2 \in \ker f$ then $f(v_1 + v_2) = fv_1 + fv_2 = 0 + 0 = 0$, whence $v_1 + v_2 \in \ker f$, and it follows that $\ker f$ is closed under addition. If $v \in \ker f$ and $\lambda \in F$ then $f(\lambda v) = \lambda(fv) = \lambda 0 = 0$, and it follows that $\ker f$ is closed under scalar multiplication. So $\ker f$ is vector subspace of V. Furthermore, $\ker f$ is closed under the G-action, since if $v \in \ker f$ and $g \in G$ then $f(gv) = g(fv) = g0 = 0$, where the last step follows from the fact that $x \mapsto gx$ is a linear map $V \to V$ and must therefore take 0 to 0.

The proof that $\operatorname{im} f$ is a submodule of W is equally easy. If w_1, $w_2 \in \operatorname{im} f$ then $w_1 = fv_1$ and $w_2 = fv_2$ for some $v_i \in V$, and since $w_1 + w_2 = fv_1 + fv_2 = f(v_1 + v_2)$ it follows that $\operatorname{im} f$ is closed under addition. Closure under scalar multiplication and the G-action are equally easy: if $w = fv \in \operatorname{im} f$ then for all $\lambda \in F$ we have $\lambda w = f(\lambda v) \in \operatorname{im} f$, and for all $g \in G$ we have $gw = g(fv) = f(gv) \in \operatorname{im} f$. And $\operatorname{im} f \neq \emptyset$ since $V \neq \emptyset$. So $\operatorname{im} f$ is a submodule of W.

Because $\ker f$ is a submodule of V the quotient module $V/\ker f$ exists. We need to show that there is a well-defined map $\psi: V/\ker f \to \operatorname{im} f$ such that $\psi(v + \ker f) = fv$ for all $v \in V$. It is certainly true that $fv \in \operatorname{im} f$ for all v, and so we need only to show that if v_1, $v_2 \in V$ with $v_1 + \ker f = v_2 + \ker f$ then $fv_1 = fv_2$. But this is clear: if $v_1 + \ker f = v_2 + \ker f$ then $v_1 - v_2 \in \ker f$; so $f(v_1 - v_2) = 0$, and hence $fv_1 = fv_2$.

Having established that ψ is well-defined, it remains to show that it is bijective and respects addition, scalar multiplication and the action of G. The latter point follows immediately from the fact that f respects addition, scalar multiplication and the action of G. Explicitly, if u, $v \in V$ and $\lambda \in F$ then

$$\psi((u + \ker f) + (v + \ker f)) = \psi((u + v) + \ker f) = f(u + v) = fu + fv = \psi(u + \ker f) + \psi(v + \ker f)$$

and

$$\psi(\lambda(v + \ker f)) = \psi(\lambda v + \ker f) = f(\lambda v) = \lambda(fv) = \lambda\psi(v + \ker f),$$

and similarly if $g \in G$,

$$\psi(g(v + \ker f)) = \psi(gv + \ker f) = f(gv) = g(fv) = g\psi(v + \ker f).$$

Surjectivity of ψ is obvious: by definition every element of $\operatorname{im} f$ has the form $fv = \psi(v + \ker f)$ for some $v \in V$. And injectivity is not much harder: if $\psi(v_1 + \ker f) = \psi(v_2 + \ker f)$ then $fv_1 = fv_2$, whence $f(v_1 - v_2) = 0$, which yields that $v_1 - v_2 \in \ker f$, and hence $v_1 + \ker f = v_2 + \ker f$.

Indecomposable and irreducible modules

Recall that a vector space V is said to be the *internal direct sum* of its subspaces X and Y if every element of V is uniquely expressible in the form $x + y$ with $x \in X$ and $y \in Y$. We call this a *direct decomposition* of V, and we write $V = X \oplus Y$. We also say that X and Y are *complementary subspaces* of V. It is easily seen that if $V = X \oplus Y$ then $V/X \cong Y$, an isomorphism $Y \to V/X$ being given by $y \mapsto y + X$ for all $y \in Y$. (The symbol "$\cong$" means "is isomorphic to".)

In terms of bases, a direct decomposition of a vector space amounts to splitting a basis into two pieces; thus if $V = X \oplus Y$ then if $x_1, x_2, \ldots, x_n$ is a basis for X and $y_1, y_2, \ldots, y_m$ a basis of Y then $x_1, \ldots, x_n, y_1, \ldots, y_m$ is a basis of V. It is a basic theorem of vector space theory that a basis of a subspace can always be extended to a basis of V. Thus if X is a subspace of V and $x_1, x_2, \ldots, x_n$ is a basis of X then there exist $x_{n+1}, x_{n+2}, \ldots, x_d$ such that $x_1, x_2, \ldots, x_d$ is a basis of V. The subspace Y of V that is spanned by $x_{n+1}, x_{n+2}, \ldots, x_d$ is then complementary to X, and we obtain the important fact that for every subspace X of a vector space V there is subspace Y of V such that $V = X \oplus Y$. Indeed, there are usually many subspaces Y complementing a given X.

The direct decomposition concept generalizes easily to G-modules. A G-module V is the G-module direct sum of X and Y if X and Y are G-submodules of V and $V = X \oplus Y$ as vector spaces. If $V = X \oplus Y$ (where X and Y are G-submodules) then $Y \cong_G V/X$, where we have attached a subscript G to the isomorphism sign to indicate that this is a G-isomorphism (an isomorphism of G-modules). As before, the mapping ψ from Y to V/X given by $\psi y = y + X$ is an isomorphism. We already know that it is a vector space isomorphism, and so we only need to check that it respects the G action. This is immediate from the definition of the action of G on X/Y: for all $y \in Y$ and $g \in G$,

$$\psi(gy) = gy + X = g(y + X) = g(\psi y).$$

However, it is not at all clear that for every G-submodule X of a G-module V there is a complementary submodule. Since a submodule is *a fortiori* a vector subspace, there will be a complementary subspace, but among all such complements is there one which is G-invariant? (Note that vetor subspace of a G-module is said to be G-invariant if and only if it is closed under the G-action; thus a G-invariant subspace of V is the same thing as a G-submodule of V.)

It is not true in general that for every group G and every G-module V, every G-invariant subspace has a G-invariant complement. For example, consider the group G consisting of all 2×2 matrices over F of the form $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, where λ is arbitrary. In fact G is isomorphic to the additive group of F via the mapping $\phi\colon \lambda \mapsto \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$: this mapping is clearly bijective, and

$$\phi(\lambda + \mu) = \begin{pmatrix} 1 & \lambda + \mu \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} = (\phi\lambda)(\phi\mu).$$

But what is more to the point at present is that the space V of all two-component column vectors is a G-module which has only one proper submodule, namely the subspace X consisting of all two-component vectors whose second component is 0. For suppose that U is another nonzero submodule of V. Then U contains a nonzero column vector $\begin{pmatrix} x \\ y \end{pmatrix}$. Since U is closed under that action of G we deduce that

$$\begin{pmatrix} x + \lambda y \\ y \end{pmatrix} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \in U$$

for all $\lambda \in F$, and by closure of U under subtraction

$$\begin{pmatrix} \lambda y \\ 0 \end{pmatrix} = \begin{pmatrix} x + \lambda y \\ y \end{pmatrix} - \begin{pmatrix} x \\ y \end{pmatrix} \in U$$

for all $\lambda \in F$. In particular, if $y \neq 0$ then by taking $\lambda = y^{-1}$ we deduce that U contains $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and hence (by closure under scalar multiplication) all vectors whose second component is 0. On the other hand, if $y = 0$ then x must be nonzero (since we assumed that $\begin{pmatrix} x \\ y \end{pmatrix}$ is nonzero), and the same conclusion follows since now the scalar multiples of $\begin{pmatrix} x \\ y \end{pmatrix}$ give all vectors which are zero in the second component. So the submodule U contains X (which is already enough to show that U cannot be a complement to X). If U is not equal to X then it must contain some vector which is nonzero in the seond component, and since this vector together with $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (which is in X and hence in U) span V it follows that U equals the whole of V.

Definition. (i) A G-module V is said to be *indecomposable* if it cannot be expressed as a direct sum of two nonzero submodules.

(ii) A G-module V is said to be *irreducible* if it has no submodules other than itself and the zero submodule.

We have given above an example of a module V which is indecomposable but not irreducible. As a vector space V is two-dimensional, and it has a submodule which was one-dimensional as a vector space; this shows that V is not irreducible. But since V has no other nontrivial submodules it cannot be expressed as a direct sum of two nontrivial submodules; hence it is indecomposable. The first main result of representation theory that we intend to prove is the famous theorem of Maschke which asserts that if the group G is finite and the order of G is nonzero as an element of F then every indecomposable G-module is irreducible.*

* How could the order of G be zero in F? The point is that some fields satisfy unusual equations like $1+1=0$ or $1+1+1=0$. So it may be that a nonzero integer n becomes zero when interpreted as an element of F. If this happens then the least such positive integer is called the *characteristic* of F. The hypothesis of Maschke's theorem can thus be rephrased as follows: G must be finite and the characteristic of F should not be a divisor of $|G|$. So, for example, if we took G to be the group S_3 of order 6, and F to be the integers modulo 3, then $1+1+1=0$, whence $6=0$ in F, and Maschke's theorem would not apply.