Notes on Molien's Theorem

J.M. Selig
Faculty of Business, Computing and Information Management,
London South Bank University,
London SE1 0AA, UK

June 23, 2006

1 Introduction—a finite group

Molien's theorem concerns the invariants of finite groups. So we will introduce a small finite group to use for our examples.

The permutation group or symmetric group on 3 letters has the presentation,

$$S_3 =< \sigma, \tau \,|\, \sigma^2 = \tau^3 = e, \sigma\tau = \tau^2\sigma >$$

that is, σ and τ are generators of the group, e being the identity element. These generators satisfy the relations, $\sigma^2 = \tau^3 = e$, that is σ has order 2 and τ order 3, in fact σ can be thought of as a swap and τ as a cycle. The final relation is $\sigma\tau = \tau^2\sigma$, or $\sigma\tau\sigma = \tau^3$ which shows that the subgroup generated by τ on its own is a normal subgroup.

In cycle notation we could write,

$$\sigma = (12), \quad \tau = (123).$$

2 Representations

We begin with a formal definition of a representation.

Definition 1 *Representation A representation of a finite group G is a homomorphism,*

$$R : G \longrightarrow \hom(V, V).$$

Here $\hom(V, V)$ is the space of homomorphisms from a vector space V to itself. The dimension of the vector space V is known as the dimension of the representation.

Once we have chosen a basis for V the elements of $\hom(V, V)$ can be interpreted as $n \times n$ matrices, where n is the dimension of the representation. The condition that the representation must be a homomorphism now becomes the condition,

$$R(g_1)R(g_2) = R(g_1g_2), \quad \text{for all } g_1, g_2 \in G.$$

The multiplication on the left is matrix multiplication while the product on the right of this equation is multiplication in the group. This condition has the simple consequence that,

$$R(g^{-1}) = R(g)^{-1},$$

the matrix representing the inverse of an element is the inverse of the matrix representing the original group element. And hence,

$$R(e) = I,$$

the matrix representing the identity element is always the identity matrix.

If we had chosen a different basis for V we would have got a different set of matrices, but from the definition above the same representation. In fact if the two bases are related by a non-singular matrix M then the new matrix representation will have elements,

$$R'(g) = MR(g)M^{-1}.$$

So we introduce an equivalence relation between representations $R' \simeq R$ if the above relation is satisfied for all $g \in G$.

Finally in this section some examples of representations of S_3.

(i) **The trivial representation**. For any group, the trivial representation is given by $T(g) = 1$ for all $g \in G$.

(ii) **The alternating representation**. We can find an alternating representation for any symmetric group. We set,

$$A(\sigma) = -1, \quad A(\tau) = 1.$$

Notice we only have to define the representation for the generators of the group since the homomorphism property will give us the values for other group elements. In this representation even permutations are represented by 1 and odd ones by -1. Both the trivial and alternating representations are 1 dimensional.

(iii) **The permutation representation**. Here we represent permutations by their corresponding permutation matrices,

$$P(\sigma) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad P(\tau) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

3 Direct Sums of Representations

Given two representations $A : G \longrightarrow \hom(V_1, V_1)$ and $B : G \longrightarrow \hom(V_2, V_2)$ of a group G we can produce another representation on the vector space $V_1 \oplus V_2$. In terms of matrices this new representation, the direct sum of the two original representations, can be written in partitioned form as,

$$A \oplus B(g) = \begin{pmatrix} A(g) & 0 \\ 0 & B(g) \end{pmatrix}, \quad \text{for all } g \in G.$$

Notice that V_1 and V_2 are both invariant subspaces of this new representation. That is for any $\mathbf{v} \in V_1$ and any $g \in G$ the result of the product $A \oplus B(g)\mathbf{v}$ lies in V_1 and similar for V_2. This is easily seen if we identify V_1 and V_2 with vectors of the form,

$$\begin{pmatrix} \mathbf{v} \\ \mathbf{0} \end{pmatrix} \in V_1 \quad \text{and} \quad \begin{pmatrix} \mathbf{0} \\ \mathbf{u} \end{pmatrix} \in V_2.$$

Of course, if a representation doesn't have the block diagonal form shown above doesn't mean it is not a direct sum of representations since it might be possible to find a non-singular matrix M which block diagonalises the representation. That is the representation may be equivalent to a direct sum. We will see an example of this in a moment first a useful technical result.

Lemma 1 *Let $R : G \longrightarrow \hom(V, V)$ be a representation and suppose $U \subseteq V$ is an invariant subspace then there is a complementary invariant subspace $W \subseteq V$ such that $V = W \oplus U$.*

To prove this we introduce the averaging operator X,

$$X = \frac{1}{|G|} \sum_{g \in G} R(g).$$

This is a sum over all group elements and depends on the representation, so we should really write X_R, or something similar, but the representation will always fixed when we use this so no confusion should arise. Now this operator is a linear map from V to V and if $\mathbf{u}$ lies in an invariant subspace of V then so will $X\mathbf{u}$. This follows from the fact that for all $h \in G$,

$$R(h)X = XR(h) = X.$$

Since X is a sum over all group elements multiplying by $R(h)$ just reorders the sum,

$$R(h)X = \frac{1}{|G|} \sum_{g \in G} R(h)R(g) = \frac{1}{|G|} \sum_{g \in G} R(hg) = \frac{1}{|G|} \sum_{g' \in G} R(g') = X.$$

Now we can see easily that $XR(h)\mathbf{u} = R(h)X\mathbf{u}$ and hence X does indeed preserve invariant subspaces. In fact for any vector $\mathbf{v}$ the product $X\mathbf{v}$ will be invariant since,

$$R(h)X\mathbf{v} = X\mathbf{v}.$$

Next we see that the kernel of X is also an invariant subspace, since,

$$X\mathbf{w} = \mathbf{0} \quad \Rightarrow \quad XR(h)\mathbf{w} = R(h)X\mathbf{w} = \mathbf{0}.$$

So we may identify, $W = \ker(X)$ since any vector is either in the kernel of X or projected to the invariant subspace by X.

Note that this result can be proved in other ways and can also be generalised to semi-simple Lie groups but not to more general Lie groups.

Finally here the promised example. Consider the permutation representation od S_3. This has an invariant subspace,

$$P(\sigma)\begin{pmatrix}1\\1\\1\end{pmatrix}=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}1\\1\\1\end{pmatrix}=\begin{pmatrix}1\\1\\1\end{pmatrix}$$

and

$$P(\tau)\begin{pmatrix}1\\1\\1\end{pmatrix}=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\begin{pmatrix}1\\1\\1\end{pmatrix}=\begin{pmatrix}1\\1\\1\end{pmatrix}$$

Notice we only need to check this on the generators. So the vector $(1,1,1)^T$ generates a 1-dimensional invariant subspace. This means that the permutation representation is really a direct sum $P \simeq D \oplus T$, where T is the trivial representation and D turns out to be the 2-dimensional representation,

$$D(\sigma)=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad D(\tau)=\begin{pmatrix}-\frac{1}{2}&i\frac{\sqrt{3}}{2}\\-i\frac{\sqrt{3}}{2}&-\frac{1}{2}\end{pmatrix}.$$

4 Linear Invariants

An invariant is pretty much what you would expect it to be: something left unchanged by the action of the group. However we will approach this slowly, defining first linear invariants.

Definition 2 *Linear Invariants A linear invariant* $\mathbf{j}$ *is a linear map* $\mathbf{j} : V \longrightarrow \mathbb{C}$ *which satisfies:*

$$\mathbf{j}\big(R(g)\mathbf{v}\big)=\mathbf{j}(\mathbf{v}),\quad \textit{for all } g\in G \quad \textit{and all } \mathbf{v}\in V.$$

Again this definition is relative to a particular representation, but the notation will assume that the representation is understood.

As an example we look at the permutation representation again. Here $V=\mathbb{C}^3$ and element of this space can be written as column vectors,

$$\mathbf{v}=\begin{pmatrix}x\\y\\z\end{pmatrix}.$$

A linear function, or functional, on these vectors can be written as a vector,

$$\mathbf{j}(\mathbf{v})=\mathbf{j}^T\mathbf{v}=(a,\,b,\,c)\begin{pmatrix}x\\y\\z\end{pmatrix}=ax+by+cz.$$

Formally the vectors $\mathbf{j}$ are elements of the vector space dual to V, that is $\hom(V,\mathbb{C})$; usually written V^*. Now the condition for a linear invariant given above becomes,

$$\mathbf{j}^T R(g)\mathbf{v}=\mathbf{j}^T R(g)\mathbf{v},\quad \text{for all } g\in G \quad \text{and all } \mathbf{v}\in V.$$

Since this must hold for all $\mathbf{v}$ we can rewrite it as,

$$R^T(g)\mathbf{j} = \mathbf{j}, \quad \text{for all } g \in G.$$

For the permutation representation we have,

$$P^T(g) \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \quad \text{for all } g \in S_3.$$

Notice that we are looking for 1-dimensional invariant subspaces of the representation P^T equivalent to the trivial representation. The representation P^T is the dual of the original representation P. For the above we have the solution $a = b = c$ and hence the invariant $\mu(x + y + z)$ where μ is some constant. The question is are there any other invariants? Certainly if we had two invariants, $\mathbf{j}_1$ and $\mathbf{j}_2$ then any linear combination, $\mu\mathbf{j}_1 + \lambda\mathbf{j}_2$ would also be an invariant so we are really asking for the number of linearly independent linear invariants.

Lemma 2 *The number of linearly independent linear invariants is given by,*

$$\mathrm{Tr}(X) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\left(R^T(g)\right),$$

where Tr *denotes the trace of the operator.*

To show this we consider the averaging operator,

$$X = \frac{1}{|G|} \sum_{g \in G} R^T(g).$$

This is the averaging operator relative to the dual of the original representation R. So this X is the transpose of the X defined in the previous section. However, since the representation was fixed but arbitrary in the previous section its properties remain the same, in particular $R^T(h)X = X$ for all $h \in G$. Now let $\mathbf{l} \in V^*$ be an arbitrary linear functional. Then if $X\mathbf{l}$ is not zero it is an invariant since $R^T(h)X\mathbf{l} = X\mathbf{l}$ for all $h \in G$. This means that X must be equivalent to a diagonal matrix of 1s and 0s,.

$$X \simeq \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

Each 1 on the diagonal corresponds to a linearly independent invariant so the trace of this matrix count the number of linearly independent linear invariants, and $\mathrm{Tr}(MXM^{-1}) = \mathrm{Tr}(XM^{-1}M) = \mathrm{Tr}(X)$. Finally, the trace is a linear operator so the trace of a sum

is the sum of the traces and hence the result. Notice that the transpose in the formula above is really irrelevant since $\mathrm{Tr}(A^T) = \mathrm{Tr}(A)$ for any square matrix, it has been included in the above simply to remind us that it is the dual of the original representation we are using.

Returning to our example, we can evaluate the sum a little more efficiently by noticing that the trace is constant on a conjugacy class. The group S_3 has 3 conjugacy classes, the first containing only the identity has $\mathrm{Tr}\big(P(e)\big) = 3$. The second conjugacy class contains the 3 swaps σ, $\sigma\tau$ and $\sigma\tau^2$, these have $\mathrm{Tr}\big(P(\sigma)\big) = 1$. Lastly the cycles τ and τ^2 have trace $\mathrm{Tr}\big(P(\tau)\big) = 0$. So we have,

$$\mathrm{Tr}(X) = \frac{1}{|S_3|}\sum_{g\in S_3}\mathrm{Tr}\big(P(g)\big) = \frac{1}{6}(3 + 3\times 1 + 2\times 0) = 1.$$

So $x + y + z$ is the only linear invariant, up to scalar multiples of course.

Notice that the terms $\mathrm{Tr}\big(R(g)\big)$ are just the characters of the representation. So the formula for $\mathrm{Tr}(X)$ above could be interpreted as example of the formula for the orthogonality of group characters. If $\chi_A(g) = \mathrm{Tr}\big(A(g)\big)$ and $\chi_B(g) = \mathrm{Tr}\big(B(g)\big)$ are characters of two irreducible representations A and B then,

$$\frac{1}{|G|}\sum_{g\in G}\chi_A(g)\chi_B(g) = 0.$$

Here irreducible just means that the representation has no invariant subspaces and hence cannot be decomposed into direct sums of other representations. This formula can also be used to find the number of copies of an irreducible representation in a more general one, this is given by the projection,

$$\text{no. copies of } A \text{ in } R \text{ is} = \frac{1}{|G|}\sum_{g\in G}\chi_A(g)\chi_R(g).$$

Since the characters of the trivial representation is always 1, $\chi_T(g) = 1$ for all $g \in G$, the number of copies of the trivial representation in any representation R is given by,

$$\text{no. copies of } T \text{ in } R \text{ is} = \frac{1}{|G|}\sum_{g\in G}\chi_R(g) = \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}\big(R(g)\big).$$

5 Molien's Theorem

Now we turn to polynomial invariants. The definition is almost identical to the one for linear invariants.

Definition 3 *Polynomial Invariants A polynomial invariant* $\mathbf{j}$ *is a polynomial map* $\mathbf{j} : V \longrightarrow \mathbb{C}$ *which satisfies:*

$$\mathbf{j}\big(R(g)\mathbf{v}\big) = \mathbf{j}(\mathbf{v}), \quad \textit{for all } g \in G \quad \textit{and all } \mathbf{v} \in V.$$

By a polynomial map here we mean a map that is a polynomial in the components of $\mathbf{v}$. The action of the group G on these polynomial functions preserves the total degree of the polynomial so we only have to consider homogeneous polynomial invariants, any polynomial invariant can be decomposed into a sum of homogeneous polynomial invariants. From now on a homogeneous polynomial invariant will be referred to simply as an invariant.

As a simple example we look at degree 2, or quadratic, invariants of a 3-dimensional representation $R : G \longrightarrow \hom(\mathbb{C}^3, \mathbb{C}^3)$. If the components of $\mathbf{v} \in \mathbb{C}^3$ are $\mathbf{v}^T = (x,\, y,\, z)$ then a quadratic function will have the form,

$$\mathbf{j}(\mathbf{v}) = ax^2 + 2bxy + 2cxz + dy^2 + 2eyz + fz^2.$$

The 2 in the definition above are so that we can write this neatly as a matrix product,

$$\mathbf{j}(\mathbf{v}) = \mathbf{v}^T A \mathbf{v} = (x,\, y,\, z) \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

where,

$$A = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}.$$

So the quadratic invariants must satisfy,

$$R^T(g) A R(g) = A, \quad \text{for all } g \in G.$$

Notice that this matrix product $R^T A R$, defines a new representation of the group on the vector space of symmetric 3×3 matrices, the As. This representation is called the symmetric square of the original representation, written $R^{\otimes_s 2}$. Actually it is the symmetric square of the dual representation but ignoring this detail will not make any significant difference in the following.

Writing the entries of A as a_{ij} and similar for the entries of $R(g)$, we can write the effect of the representation on a typical matrix entries as $\mathbf{a}' = R^{\otimes_s 2}(g)\mathbf{a}$, where the vector $\mathbf{a}$ contains the entries of A, $\mathbf{a} = (a_{11},\, a_{12},\, a_{13},\, a_{22},\, a_{23},\, a_{33})^T$. The elements of $R^{\otimes_s 2}(g)$ are then given by,

$$\begin{pmatrix} r_{11}^2 & 2r_{11}r_{21} & 2r_{11}r_{31} & r_{21}^2 & 2r_{21}r_{31} & r_{31}^2 \\ r_{11}r_{12} & r_{12}r_{21} + r_{11}r_{22} & r_{12}r_{31} + r_{11}r_{32} & r_{21}r_{22} & r_{22}r_{31} + r_{21}r_{32} & r_{31}r_{32} \\ r_{11}r_{13} & r_{13}r_{21} + r_{11}r_{23} & r_{13}r_{31} + r_{11}r_{33} & r_{21}r_{23} & r_{23}r_{31} + r_{21}r_{33} & r_{31}r_{33} \\ r_{12}^2 & 2r_{12}r_{22} & 2r_{12}r_{32} & r_{22}^2 & 2r_{22}r_{32} & r_{32}^2 \\ r_{12}r_{13} & r_{13}r_{22} + r_{12}r_{23} & r_{13}r_{32} + r_{12}r_{33} & r_{22}r_{23} & r_{23}r_{32} + r_{22}r_{33} & r_{32}r_{33} \\ r_{13}^2 & 2r_{13}r_{23} & 2r_{13}r_{33} & r_{23}^2 & 2r_{23}r_{33} & r_{33}^2 \end{pmatrix}$$

We can count the number of linearly independent quadratic invariants using the formula from the last section but substituting this representation,

$$\text{No. quadratic invariants} = \frac{1}{|G|} \sum_{g \in G} \text{Tr}\left(R^{\otimes_s 2}(g)\right).$$

Finding all the elements of the representation when all we need is the trace is rather inefficient so we assume that we can choose coordinates in V so that $R(g)$ is diagonal. The diagonal elements will be the eigenvalues of the matrix of course. Suppose that these eigenvalues are w_1, w_2 and w_3, the action of the matrix on the coefficients will be given by,

$$a'_{ij} = a_{ij} w_i w_j$$

and hence the trace of the matrix $R^{\otimes_s 2}(g)$ will be given by,

$$\mathrm{Tr}\left(R^{\otimes_s 2}(g)\right) = \sum_{1 \leq i \leq j \leq 3} w_i w_j = w_1^2 + w_1 w_2 + w_1 w_3 + w_2^2 + w_2 w_3 + w_3^3.$$

Notice that we have to be careful here to restrict the sum to the values $1 \leq i \leq j \leq 3$, so that we don't count the coefficients of a_{ij} and a_{ji} as different. Also notice that whether or not $R(g)$ is diagonalisable or not is actually not important. The argument above is just a quick way to produce the formula for the trace of the matrix $R^{\otimes_s 2}(g)$ in terms of the eigenvalues of $R(g)$, it will not depend on whether or not we can actually diagonalise $R(g)$.

For our permutation example we have,

$$\mathrm{Tr}\left(P^{\otimes_s 2}(e)\right) = 6,$$

since, $P(e)$ has eigenvalues $w_1 = w_2 = w_3 = 1$.

$$\mathrm{Tr}\left(P^{\otimes_s 2}(\sigma)\right) = 2,$$

since $P(\sigma)$ has eigenvalues $w_1 = w_2 = 1$ and $w_3 = -1$. Lastly,

$$\mathrm{Tr}\left(P^{\otimes_s 2}(\tau)\right) = 0,$$

since $P(\tau)$ has eigenvalues $w_1 = 1$, $w_2 = \omega$ and $w_3 = \omega^2$ where ω is a cube root of unity; $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. The relation $1 + \omega + \omega^2 = 0$ is useful here.

The number of quadratic invariants is therefore,

$$\frac{1}{6} \sum_{g \in S_3} \mathrm{Tr}\left(P^{\otimes_s 2}(g)\right) = \frac{1}{6}(6 + 3 \times 2 + 2 \times 0) = 2.$$

So there are two quadratic invariants, one is clearly, $(x + y + z)^2$, the square of the linear invariants. The other is $x^2 + y^2 + z^2$ or some linear combination of these two invariants.

More generally, if R is a representation on an n-dimensional vector space with coordinates x_1, $x_2, \ldots, x_n$, then the degree d invariants are given by,

$$\mathbf{j}(\mathbf{v}) = \sum_{i_1, i_2, \ldots i_d = 1}^{n} A_{i_1, i_2, \ldots i_d} x_{i_1} x_{i_2} \cdots x_{i_d},$$

subject to the condition that,

$$A_{i_1, i_2, \ldots i_d} = \sum_{j_1, j_2, \ldots j_d = 1}^{n} A_{j_1, j_2, \ldots j_d} R_{j_1, i_1}(g) R_{j_2, i_2}(g) \cdots R_{j_d, i_d}(g),$$

for all $g \in G$, and $1 \leq i_1, i_2, \ldots i_d \leq n$. The $A_{i_1,i_2,\ldots i_d}$ here is the tensor of coefficients. The action of the group on this tensor is called the symmetric d-fold power of the original representation $R^{\otimes_s d}$. If we use a basis in which $R(g)$ is diagonal with eigenvalues $w_1,\ w_2, \ldots, w_n$ the trace of the symmetric d-fold power is given by,

$$\mathrm{Tr}\left(R^{\otimes_s d}(g)\right) = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_d \leq n} w_{i_1} w_{i_2} \cdots w_{i_d}.$$

Now at last we can give Molien's theorem.

Theorem 1 *(Molien 1898) Suppose that a_d is the number of linearly independent homogeneous invariants of G with degree d and let,*

$$\Phi(\lambda) = \sum_{d=0}^{\infty} a_d \lambda^d$$

be the generating function for this sequence, then,

$$\Phi(\lambda) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det\left(I - \lambda R(g)\right)}.$$

The number of degree d invariants a_d, is given by the sum of the traces of the matrices in the d-fold symmetric power representation,

$$a_d = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}\left(R^{\otimes_s d}(g)\right),$$

since the degree-d invariants are linear invariants for this representation. To prove the theorem all we need to do is to compare this sum with the one given in the theorem. If fact we can just compare terms, for some particular $g \in G$ we have

$$\mathrm{Tr}\left(R^{\otimes_s d}(g)\right) = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_d \leq n} w_{i_1} w_{i_2} \cdots w_{i_d}.$$

The corresponding term in the other sum is the coefficient of λ^d in,

$$\frac{1}{\det\left(I - \lambda R(g)\right)} = \frac{1}{(1 - \lambda w_1)(1 - \lambda w_2) \cdots (1 - \lambda w_n)},$$

where the determinant has been expanded in terms of the eigenvalues of $R(g)$. Expanding the expression on the right-hand side here gives,

$$\frac{1}{(1 - \lambda w_1)(1 - \lambda w_2) \cdots (1 - \lambda w_n)} =$$

$$(1 + \lambda w_1 + \lambda^2 w_1^2 + \cdots)(1 + \lambda w_2 + \lambda^2 w_2^2 + \cdots) \cdots (1 + \lambda w_n + \lambda^2 w_n^2 + \cdots),$$

the coefficient of λ^d in this expression can be seen to be,

$$\sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_d \leq n} w_{i_1} w_{i_2} \cdots w_{i_d},$$

as above, hence the theorem is proved.

Our example will be the permutation representation of S_3 as usual. Again we can simplify the calculation a little using the fact that $\det\big(I - \lambda R(g)\big)$ is constant on a conjugacy class. So we have,

$$\det\big(I - \lambda P(e)\big) = \det\begin{pmatrix} 1-\lambda & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & 1-\lambda \end{pmatrix} = (1-\lambda)^3,$$

then,

$$\det\big(I - \lambda P(\sigma)\big) = \det\begin{pmatrix} 1 & -\lambda & 0 \\ -\lambda & 1 & 0 \\ 0 & 0 & 1-\lambda \end{pmatrix} = (1-\lambda)(1-\lambda^2),$$

and finally,

$$\det\big(I - \lambda P(\tau)\big) = \det\begin{pmatrix} 1 & -\lambda & 0 \\ 0 & 1 & -\lambda \\ -\lambda & 0 & 1 \end{pmatrix} = (1-\lambda^3).$$

Assembling these results gives,

$$\begin{aligned} \frac{1}{|S_3|}\sum_{g\in S_3}\frac{1}{\det\big(I-\lambda P(g)\big)} &= \frac{1}{6}\left(\frac{1}{(1-\lambda)^3} + \frac{3}{(1-\lambda)(1-\lambda^2)} + \frac{2}{(1-\lambda^3)}\right) \\ &= \frac{(1-\lambda^2)(1-\lambda^3) + 3(1-\lambda)^2(1-\lambda^3) + 2(1-\lambda)^3(1-\lambda^2)}{6(1-\lambda)^3(1-\lambda^2)(1-\lambda^3)} \\ &= \frac{1}{(1-\lambda)(1-\lambda^2)(1-\lambda^3)} \end{aligned}$$

So,

$$\Phi(\lambda) = \frac{1}{(1-\lambda)(1-\lambda^2)(1-\lambda^3)},$$

this means that the ring of invariants is generated by three elements, a linear invariant a degree 2 invariant and a degree 3 invariant. To see this in detail we can expand the first few terms in the generating function,

$$\begin{aligned} \Phi(\lambda) &= (1+\lambda+\lambda^2+\cdots)(1+\lambda^2+\lambda^4+\cdots)(1+\lambda^3+\lambda^6+\cdots) \\ &= 1+\lambda+2\lambda^3+3\lambda^3+4\lambda^4+\cdots \end{aligned}$$

So this is one linear invariant, as we have seen this is $I_1 = x+y+z$. There are two degree 2 invariants, one must be $I_1^2 = (x+y+z)^2$ the square of the linear invariant. The other is a new invariant which could be $I_2 = x^2+y^2+z^2$ or $xy+yz+zx$ but not both since these are not linearly independent $I_1^2 - I_2 = 2(xy+yz+zx)$. The three cubic invariants will be I_1^3, $I_1 I_2$ and a new invariant say $I_3 = x^3+y^3+z^3$. All the polynomial are now accounted for as sums and products of these three invariants, for example the four degree 4 invariants are I_1^4, $I_1^2 I_2$, I_2^2 and $I_1 I_3$.

References

This work is an attempt to explian in some more detail §III D of the following paper:

[1] N.J.A. Sloane. “Error-correcting codes and invariant theory: new application of a nineteenth-century technique”. .

The material probably appear in many other places for example,

[2] Bernd Sturmfels. *Algorithms and Invariant theory*. Springer Verlag, Wein 1993.