Some Applications of Representation Theory to Classical Number Theory

B.Sury

Indian Statistical Institute Bangalore, India

E-mail: sury@ms.isibang.ac.in

These are the notes of a lecture on 'Unity of Mathematics' delivered on June 24, 2010 in an advanced instructional school on Representation Theory at the Indian Statistical Institute Bangalore.

The applications of representation theory to number theory is a subject so vast that it may be said to include the whole of the Langlands program. We do not discuss the Langlands program here but only talk briefly about the following three topics:

(I) The theory of Partitions
(II) Zeta and L-functions over number fields
(III) Kronecker-conjugacy of integer polynomials

1. The Partition Function

(Everyone knows that) Ramanujan made outstanding contributions to the theory of partitions. Ramanujan's first letter to Hardy mentions an approximate formula for $p(n)$ and Rademacher published such an exact formula soon (according to Selberg, if Hardy had been less of an analyst, Ramanujan's approximate formula might have been realized to quickly lead to an exact formula). Hardy and Ramanujan developed the so-called circle method and published asymptotic formulae like

$$p(n) \sim \frac{e^{2\sqrt{n\zeta(2)}}}{4\sqrt{3}n}.$$

Here, the crucial thing to note is the exponent $2\sqrt{\zeta(2)}$ which is approximately 2.56.

From a point of view of the actual values of $p(n)$, for small n, these values are much smaller than the asymptotic values. Representation theory especially of the symmetric group plays a role here to provide easy but close lower bounds for $p(n)$. Let us discuss this first. All relevant background information on partition theory as well as much more historical and other material for the interested reader can be found in [1], and [2]. For the basic results on representation theory, one may refer to [9] or the classic [15]. Let us start with an elementary lemma.

Lemma. *Let* $\mathrm{Inv}(G)$ *denote the set of involutions of a finite group* G*. Then,*

$$\sum_{\chi \in \mathrm{Irr}(G)} \nu_2(\chi)\dim(\chi) = 1 + |\mathrm{Inv}(G)|$$

where $\nu_2(\chi) = 0, 1,$ *or* -1 *according as to whether the character* χ *is not real-valued, or, is real-valued and afforded by a real representation or, is real-valued but not afforded by a real representation. This* ν_2 *is the so-called Frobenius-Schur indicator function.*

In fact, for each n, expressing the class function

$$\theta_n(g) = |\{x : x^n = g\}|$$

as $\theta_n = \sum_{\chi \text{ irr}} \nu_n(\chi)\chi$ obtains

$$\nu_n(\chi) = \langle \theta_n, \chi \rangle = \frac{1}{O(G)} \sum_g \chi(g^n)$$

for each irreducible χ. In the special case $n = 2$, we have

$$|\mathrm{Inv}(G)| + 1 = \theta_2(1) = \sum_{\chi \text{ irr}} \nu_2(\chi)\chi(1)$$

The values $0, 1, -1$ of $\nu_2(\chi)$ are obtained by decomposing the representation space of χ into its symmetric and antisymmetric parts.

As $\nu_2(\chi) = \langle \theta_2, \chi \rangle$, we have

$$1 + |\mathrm{Inv}(G)| = \sum_{\chi \text{ irr}} \nu_2(\chi)\chi(1) = \langle \theta_2, \chi_{\mathrm{reg}} \rangle$$

Therefore, from the Cauchy-Schwarz inequality we have

$$|\mathrm{Inv}(G)| < \sqrt{r(G)}\sqrt{O(G)}$$

where $r(G)$ is the number of irreducible characters afforded by real representations. In particular, since $r(G) \leq k(G)$, the number of conjugacy classes of G, we have

$$\frac{O(G)}{O(C_G(g))^2} < k(G)$$

where g is any involution.

Corollary. $\frac{e^{2\sqrt{n}}}{cn} < p(n)$ *for some constant* c.

Proof. Apply the lemma to S_n. Now $f(n,t) = \frac{n!}{2^t t!(n-2t)!}$ is the number of involutions of S_n which are products of t disjoint transpositions. The lemma gives

$$p(n) = k(S_n) > \frac{|\mathrm{Inv}(S_n)|^2}{n!}$$
$$= \frac{\left(\sum_{t=1}^{[n/2]} f(n,t)\right)^2}{n!} > \sum_{t=1}^{[n/2]} \frac{f(n,t)^2}{n!}.$$

We can easily see from $\frac{f(n,t)}{f(n,t+1)} = \frac{2(t+1)}{(n-2t)(n-2t-1)}$ that $f(n,t) \leq f(n,t+1)$ if and only if $(n-2t)^2 \geq n+2$. Therefore, the largest value of $f(n,t)$ for $t \leq n/2$ is when $t = [(n+2-\sqrt{n+2})/2]$. Using Stirling's formula we get the assertion of the corollary. A more careful argument on the above lines shows that one can take $c = e^3\sqrt{2\pi^3}$.

Remarks.

(i) The above proof can be combinatorially viewed via the Robinson-Schensted algorithm. This algorithm provides a bijection between S_n and pairs of standard tableaux of the same shape. In particular, it gives $n! = \sum_{\lambda \vdash n} a_\lambda^2$ where a_λ is the number of tableaux of shape $\lambda \vdash n$. Under this correspondence, elements of order ≤ 2 are in correspondence with pairs of tableaux with identical entries. Hence $\sum_{\lambda \vdash n} a_\lambda = 1 + |\mathrm{Inv}(S_n)|$. The arithmetic mean – quadratic mean inequality for the a_λ's gives the result now.

(ii) This estimate is close to the general size of $p(n)$ because most irreducible character degrees of S_n are nearly equal.

As the irreducible (complex) representations of S_n are parametrized by partitions, let χ_λ denote the character corresponding to a partition λ of n. Using the theory of blocks – especially using the recent generalization ([10]) of Nakayama's conjecture connecting combinatorial blocks to the blocks of modular representation theory – one can prove the following result on partitions. We do not go into its proof here.

Theorem. *For all* $d \leq n$, *we have* $p(n) \geq p([n/d^2])^d$.

If $d = [\sqrt{n/2}]$, this gives $p(n) \geq 2^{[\sqrt{n/2}]}$ but one can derive the stronger consequence:

Corollary. $p(n) > \frac{e^{2\sqrt{n}}}{14}$.

The proof for $n < 190$ *can be checked by a computer. For slightly bigger values* $190 \leq n < 760$ *also, it can be easily checked that* $p(n) > e^{2\sqrt{n}+0.5}$. *For* $n \geq 760$, *the above theorem along with induction, gives*

$$p(n) > p([[n/2]/2])^2 > e^{4\sqrt{[[n/2]/2]}+1} > e^{2\sqrt{n}+0.5}.$$

We end by quoting the sharper lower bound $p(n) > \frac{e^{2.5\sqrt{n}}}{13n}$ *which can be deduced from the following consequence of the theory of blocks for* S_n *([11]).*

Theorem. $p(n) = \sum_{t=0}^{n} \sum_{4w+t(t+1)=2n} \sum_{l=0}^{w} p(l)p(w-l)$.

2. Zeta Functions on Number Fields

The Dedekind zeta function of an algebraic number field is an invariant which plays an important role in density theorems for ramification of primes like the Frobenius density theorem and the Chebotarev density theorem. Thus, it may be natural to expect the Dedekind zeta function to determine the number field and it comes as a surprise that it does not! In fact, a simple result from the representation theory of finite groups provides a method to construct non-isomorphic number fields with the same zeta function. These simple methods also provide a footing to discuss and prove special cases of Dedekind's conjecture asserting that for number fields $K \subset L$, the ratio $\zeta_L(s)/\zeta_K(s)$ is an entire function of s. We discuss this method here following an approach due to Robert Perlis ([13]).

Dedekind zeta function and Gassmann equivalence

The main aim of this section is to discuss a method to produce two non-isomorphic number fields with the same Dedekind zeta function. Let $N/\mathbf{Q}$ denote a finite Galois extension and write $G = \mathrm{Gal}(N/\mathbf{Q})$. If K and K' are intermediate fields, our goal is to express the equality $\zeta_K(s) = \zeta_K'(s)$ in terms of the groups G, $H := \mathrm{Gal}(N/K)$ and $H' := \mathrm{Gal}(N/K')$.

The Dedekind zeta function of an algebraic number field K is the function of the complex variable s defined in the region $\mathrm{Re}(s) > 1$ by the series $\zeta_K(s) = \sum_I 1/N(I)^s$ where I varies over non-zero integral ideals of K and $N(I)$ denotes the absolute norm (the cardinality of $\mathcal{O}_K/I$). The Dedekind zeta function has a meromorphic continuation to $\mathrm{Re}(s) > 1 - 1/[K : \mathbf{Q}]$ and has only a simple pole at the point $s = 1$.

The residue at $s = 1$ contains information about K like the class number, regulator etc.:

$$\lim_{s\to 1+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h(K)\,\mathrm{Reg}(K)}{|\mu(K)|\sqrt{|\mathrm{disc}(K)|}}.$$

For $\mathrm{Re}(s) > 1$, there is an Euler product expansion

$$\zeta_K(s) = \prod_{0\neq P \text{ prime}} (1 - N(P)^{-s})^{-1}.$$

Here, the product is over non-zero prime ideals in the ring of integers. Let $G_1(s) = (\pi)^{-s/2}\Gamma(s/2)$, $G_2(s) = (2\pi)^{1-s}\Gamma(s)$ and let r_1, r_2 denote, respectively, the numbers of real and complex places of K. Then, the completed zeta function $Z_K(s) = G_1(s)^{r_1}G_2(s)^{r_2}\zeta_K(s)$ is analytic in the whole plane except for simple poles at $s = 0, 1$ and satisfies the functional equation

$$Z_K(s) = |D_K|^{\frac{1}{2}-s}Z_K(1-s)$$

where D_K denotes the discriminant of K over $\mathbf{Q}$.

Splitting of primes

For a prime p, we will define the *splitting type of p in a number field E* as follows. Let $p\mathcal{O}_E = P_1^{e_1}\cdots P_g^{e_g}$ be the decomposition of a prime p into prime ideals in $\mathcal{O}_E$ and $f_i = [\mathcal{O}_E/P_i : \mathbf{Z}/p\mathbf{Z}]$ be the inertial degree of P_i over p. We number the f_i's in such a way that $f_i \leq f_{i+1}$ and call $(f_1, f_2, \ldots, f_g)$ the *splitting type of p in E*. For every such tuple A, we have a set

$$P_E(A) := \{p \in \mathbf{Z} : p \text{ has splitting type } A \text{ in } E\}.$$

As $\sum_{i=1}^{g} e_i f_i = [E : \mathbf{Q}]$, $P_E(A)$ is empty except for finitely many A.

We write $P_E(A) \doteq P_{E'}(A)$ if the two sets differ by at most a finite number of elements. In particular, we can exclude ramified primes as there are only finitely many of those in a number field.

Let us look at a Galois extension N and let K, K' be intermediate fields. Consider $p \in \mathbf{Z}$ which is unramified in N. Let C be a decomposition group in $G = \mathrm{Gal}(N/\mathbf{Q})$ over p in G i.e., $C = G_P$ for some prime P of N lying above p. Note C is cyclic (generated by a so-called Frobenius automorphism) as p is unramified in N.

Look at one of K, K' (say K) and let us see how a splitting type in K reflects group-theoretically in terms of G and its subgroups $H = \mathrm{Gal}(N/K)$ and $C = G_P$.

If $A = (f_1, f_2, \ldots, f_g)$ is the splitting of a prime number p in K, then we claim that there is a bijection between the set $H\backslash G/C$ of double cosets of G mod H, C and the set of prime ideals of K above p. Indeed, this is given by

$$H\sigma C \mapsto \sigma P \cap K.$$

So A is the coset type of G mod H, C. By this, we mean that the following holds good.

Writing $G = \bigcup_{i=1}^{h} Ht_iC$, we have $h = g$ and $|Ht_iC| = |H|f_i$.

This is so because Ht_iC corresponds to $t_iP \cap K$ (say P_i) and

$$|Ht_iC| = |Ht_iCt_i^{-1}| = \frac{|H||t_iCt_i^{-1}|}{|H \cap t_iCt_i^{-1}|} = \frac{|H||C|}{|H \cap t_iCt_i^{-1}|}$$

while $|C| = f_i'f_i$ where f_i', f_i are, respectively, inertial degrees of t_iP over P_i and P_i over p and $|H \cap t_iCt_i^{-1}| = |$ decomposition group of t_iP over $K| = f_i'$.

So, we conclude that p has the same splitting type in K as well as in K' if and only if the coset type of G mod $H, C =$ coset type of G mod H', C.

By the Frobenius density theorem, every cyclic subgroup C of G occurs as a decomposition group for infinitely many primes. Hence, we have:

$P_K(A) \doteq P_{K'}(A)$ for all $A \Leftrightarrow$ coset type of G mod $H, C =$ coset type of G mod H', C for all C.

Two subgroups of a finite group are said to be *Gassmann equivalent* if the permutation representations of the big group on the two coset spaces are equivalent. Note that by looking at the corresponding characters, this is equivalent to the statement that each conjugacy class in the big group intersects both subgroups in the same number of elements. This property was first studied by F. Gassmann ([8]).

The relation of this notion to double coset type is given by the:

Lemma. *Two subgroups H and H' of a finite group G are Gassmann equivalent if, and only if, the coset type of G mod $H, C =$ coset type of G mod H', C for all cyclic subgroups C of G.*

Proof. Note that each of the conditions implies $|H| = |H'|$.

Let $C = \langle c\rangle$; $c \in G$. Then

$$|HgC| = |HgCg^{-1}| = \frac{|H||C|}{|H \cap gCg^{-1}|}.$$

Look at the cardinalities l_i of the sets $\{g \in G : |HgC| = |H|i\}$.

Then, we have

$$\sum_{d|i} l_d = |\{g \in G : |HgC| \text{ divides } |H|i\}|$$
$$= |\{g \in G : H \cap \langle gcg^{-1}\rangle \supseteq \langle gc^i g^{-1}\rangle\}|$$
$$= |\{g \in G : gc^i g^{-1} \in H\}|.$$

Call the last quantity k_i.

Then, by the Möbius inversion formula $l_i = \sum_{d|i} k_d \mu(i/d)$. So, the k_i's and l_i's determine one another. As the same holds for k_i' and l_i' when H is replaced by H', it follows that the double cosets have the same decomposition types for all cyclic subgroups of G if and only if $l_i = l_i' \Leftrightarrow k_i = k_i'$. Lo and behold, this happens for every cyclic subgroup C if and only if the subgroups H and H' of G are Gassmann-equivalent.

T. Sunada constructed isospectral manifolds which are not isometric, using this property of Gassmann equivalence. This is sometimes expressed in the colourful language "one cannot hear the shape of a drum." The main theorem in our number-theoretic context here is:

Theorem. *Let K, K' be number fields contained in a Galois extension N over $\mathbf{Q}$. When $G = \mathrm{Gal}(N/\mathbf{Q})$, $H = \mathrm{Gal}(N/K)$ and $H' = \mathrm{Gal}(N/K')$, the following are equivalent:*

(a) $\zeta_K = \zeta_{K'}$.
(b) $P_K(A) = P_{K'}(A) \forall$ *tuples* A.
(c) $P_K(A) \doteq P_{K'}(A) \forall$ *tuples* A.
(d) $H = \mathrm{Gal}(N/K)$ *and* $H' = \mathrm{Gal}(N/K')$ *are Gassmann-equivalent.*

Moreover, if the above conditions hold, then the degree and the discriminants over $\mathbf{Q}$ and the numbers of real and complex places of K and K' coincide. Also, the two fields determine the same normal closures, the same normal cores (largest normal sub-extensions) and, the unit groups of K, K' are isomorphic as well.

Note that the equivalence of (c) and (d) is what we established above.

Proof of (a) implies (b). Let $A(n)$, $A'(n)$ denote the numbers of integral ideals of norm n in the rings of integers of K, K' respectively. Then

$$\zeta_K(s) = \sum_{n=1}^{\infty} A(n)/n^s, \quad \text{for} \quad \mathrm{Re}(s) > 1$$

$$\zeta_{K'}(s) = \sum_{n=1}^{\infty} A'(n)/n^s, \quad \text{for} \quad \mathrm{Re}(s) > 1.$$

Letting $s \to \infty$, we get $A(1) = A'(1)$. Cancel this term from both zeta functions, multiply by 2^s and let $s \to \infty$; we get $A(2) = A'(2)$. Repeating this argument, we have $A(n) = A'(n)$ for all n by induction.

Now, clearly the splitting type of p in K is determined by the number $B(p^f)$ of prime ideals of K of norm p^f. On the other hand,

$$B(p^f) = A(p^f) - \sum A(p^{a_1})A(p^{a_2}) \cdots A(p^{a_t})$$

where the sum is over $t \geq 2$, $a_1 + \cdots + a_t = f$. Thus the splitting types coincide for p in K and in K'. Hence, (a) implies (b).

(b) implies (c) is a tautology.
(d) implies (a):

Let C be decomposition group of the real place of $\mathbf{Q}$. Since it has order 1 or 2, it is cyclic. So, the numbers r_1, r_2 of real and complex places of K are equal to the number of double cosets Ht_iC of cardinality $|H|$ and of $2|H|$ respectively. Thus, (d) implies that the numbers r_1, r_2 are the same for K and K'.

From the completed zeta function $Z_K(s) = G_1(s)^{r_1} G_2(s)^{r_2} \zeta_K(s)$ and its functional equation

$$Z_K(s) = |D_K|^{\frac{1}{2}-s} Z_K(1-s)$$

we see that

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = |D_K/D_{K'}|^{\frac{1}{2}-s} \frac{\zeta_K(1-s)}{\zeta_{K'}(1-s)}.$$

But, the equivalence of (c) and (d) and the definition of the Dedekind zeta function as an Euler product when $\mathrm{Re}(s) > 1$ implies that the left hand side above is a finite product. That is, using (c) we have

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = \frac{\prod_{j=1}^{m}(1 - d_j^{-s})}{\prod_{j=1}^{n}(1 - c_j^{-s})}.$$

By analytic continuation above is valid for all complex s. So the conclusion would follows from the following easily proved fact asserting that finite products can not satisfy a general kind of functional equation:

Let $\tau(s) = \frac{\tau_1(s)}{\tau_2(s)}$ where $\tau_1(s) = \prod_{j=1}^{m}(1 - c_j^{-s})$ and $\tau_2(s) = \prod_{j=1}^{n}(1 - d_j^{-s})$ with c_j, d_j real and > 1. Note that $\tau_1(s)$, $\tau_2(s)$ have no poles. Let $f(s)$ be a meromorphic function whose zeroes and poles do not lie among the zeroes of

either $\tau_1(s)$ or $\tau_2(s)$. If $\tau(s) = f(s)\tau(1-s)$ for all s, then $\tau_1(s) = \tau_2(s)$ and $f(s) = 1$ for all s.

Hence we have shown that the four statements are equivalent.

Let us now assume they are true and deduce the rest of the assertions. If any of the above conditions holds then $|H| = |H'|$ which implies $[K : \mathbf{Q}] = [K' : \mathbf{Q}]$. Also, while proving the equivalence of (d) and (a), we have shown already that the numbers of real and complex places match for K, K'. Also, near the end of that proof, we observed that

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = |D_K/D_{K'}|^{\frac{1}{2}-s}\frac{\zeta_K(1-s)}{\zeta_{K'}(1-s)}.$$

Applying the above assertion on non-existence of a general functional equation for finite products, in the case of the function $f(s) = |D_K/D_{K'}|^{\frac{1}{2}-s}$. We have $f(s)$ to be identically equal to 1 and so $|D_K| = |D_{K'}|$. But the sign of the discriminant is given by the number of complex places and, therefore, the discriminants themselves are equal.

Now, the normal closure of K over $\mathbf{Q}$ is the fixed field of $\bigcap_{\sigma\in G}\sigma H\sigma^{-1}$. So, $h \in \bigcap_{\sigma\in G}\sigma H\sigma^{-1}$ implies $|\{ghg^{-1} : g \in G\}| = |\{ghg^{-1} : g \in G\} \cap H| = |\{ghg^{-1} : g \in G\} \cap H'|$ so that $h \in \bigcap_{\sigma\in G}\sigma H'\sigma^{-1}$. In other words, $\bigcap_{\sigma\in G}\sigma H\sigma^{-1} \subseteq \bigcap_{\sigma\in G}\sigma H'\sigma^{-1}$. By symmetry, the two intersections are equal and thus the normal closures of K, K' over $\mathbf{Q}$ are the same.

We will show now that the normal cores are the same as well. Note that the normal core of K over $\mathbf{Q}$ is the fixed field of the subgroup generated by all the conjugates of H in G. But, if $h \in H$, then the number of its conjugates in H' equals the number in H (which is thus non-zero). In other words, some conjugate of h is in H'. This gives that the subgroups generated by the conjugates of H and of H' are the same. Thus, the normal cores are equal.

Finally, the unit group $\mathcal{O}_K^*$ is the direct product of a free group of finite rank $r_1 + r_2 - 1$ and the finite cyclic group generated by the largest root of unity in K. The free parts are isomorphic as r_1, r_2 are equal. Now, we observe that K and K' have the same roots of unity. This is because we can adjoin largest root of unity in K to $\mathbf{Q}$ to produce a normal extension of $\mathbf{Q}$ in K' as the normal cores are the same. Thus, the unit groups are isomorphic as well. Hence the theorem is proved.

A class of examples

Here is an infinite family of examples of fields which are arithmetically equivalent but are not isomorphic.

Let H and H' be two non-isomorphic abstract groups having the same number of elements of each order – let us say then that the pair H, H' satisfies the condition $(*)$. There are infinitely many such pairs. For example, if H is an abelian group of type (p, p, p) and H' is the semi direct product of an abelian group $\langle a, b\rangle$ of type (p, p) and a cyclic group $\langle c\rangle$ of order p with $cac^{-1} = a$ and $cbc^{-1} = ab$ for some odd prime p, then H, H' satisfies $(*)$.

When H, H' is a pair satisfying $(*)$, then both H and H' can be embedded in S_n via their left regular representations, where n is their common order. Note that H is not conjugate to H' because they are not isomorphic. However, let us note that they are Gassmann-equivalent using the following lemma:

Lemma. *Elements $h, h' \in H \cup H'$ of the same order are conjugate in S_n.*

Proof. As an element of S_n, each element of H acts by multiplying the elements of H on the left and is then the product of n/i disjoint cycles of length i where $O(h) = i$. The same holds for h'. So, h and h' have same cycle structure and are thus necessarily conjugate in S_n.

Now, to show that H, H' are Gassmann-equivalent, we need to show that $|\{gcg^{-1} : g \in G\}\cap H| = |\{gcg^{-1} : g \in G\}\cap H'|$. If both intersections are empty then equality trivially holds. So, let $h \in \{gcg^{-1} : g \in G\} \cap H$. By condition $(*)$, there is some $h' \in H'$ of the same order as that of h; so h and h' are conjugate in S_n and so $h' \in \{gcg^{-1} : g \in G\} \cap H'$. Thus,

$$\{gcg^{-1} : g \in G\} \cap H = \{h \in H : O(h) = O(c)\}$$

and

$$\{gcg^{-1} : g \in G\} \cap H' = \{h' \in H' : O(h') = O(c)\}$$

which gives by condition $(*)$ that H, H' are Gassmann-equivalent.

Finally, (by Hilbert's irreducibility theorem for instance), there exists a Galois extension N of $\mathbf{Q}$ such that $\mathrm{Gal}(N/\mathbf{Q}) = S_n$. Hence, the fixed fields K and K' of H and H' are non-isomorphic but have the same zeta function.

An interesting group-theoretic result of Bart De Smit & H. W. Lenstra Jr. from 2000 ([3]) implies the following beautiful number-theoretic theorem:

Call a natural number n special if $pqr|n$ for (not necessarily distinct) primes p, q, r such that $p|q(q-1)$. Let K be a number field of degree n which is solvable by radicals. Suppose n is not special. Then, K is determined up to isomorphism by its Dedekind zeta function.

Conversely, for each special n, there are two solvable, non-isomorphic number fields of degree n which have the same Dedekind zeta function.

A key result used in the above theorem is:

Let $(n, \phi(n)) = 1$ and let X is a set of size n on which a finite, solvable group G acts transitively. Suppose G also acts on another finite set Y such that $|X^g| = |Y^g|$ for all $g \in G$ whose order is divisible only by primes dividing n. Then, X and Y are isomorphic as G-sets.

3. Value Sets of Integer Polynomials

We briefly discuss the relation of permutation representations with value sets of integer polynomials. It turns out that the concrete number-theoretic problem of deciding when two integer polynomials take the same values modulo almost all primes, is equivalent to a group-theoretic problem. Let us start with a related problem.

Can we have irreducible integer polynomials which are reducible modulo every positive integer?

More precisely, what is the relation between Galois groups of integer polynomials and the reducibility modulo primes of the polynomials?

If K is the splitting field of a monic irreducible polynomial f of degree n over $\mathbf{Z}$, then look at any prime p which does not divide the disrciminant of f. If f is irreducible modulo p, then the corresponding $\mathrm{Gal}(K/\mathbf{Q})$ contains an element of order n (a decomposition group is of order n). In other words, if $\mathrm{Gal}(K/\mathbf{Q})$ does not contain an element of order n, then f must be reducible modulo p.

In prime degrees, one cannot have monic irreducible integer polynomials which are reducible modulo all but finitely many primes. This is seen by an application of the Chebotarev (or even the) Frobenius density theorem in the following sense:

A cyclic subgroup of $\mathrm{Gal}(K/\mathbf{Q})$ *can be realized as a decomposition group over infinitely many primes.*

Therefore, if f is monic irreducible of prime degree q over integers, there are infinitely many primes p so that f mod p has splitting field with Galois group cyclic of degree q. In other words, f mod p is irreducible for infinitely many primes.

Interestingly, it turns out that for every composite degree n one may find monic irreducible integer polynomials of degree n which are reducible modulo any natural number.

However, we shall return now to the other aspect of integer polynomials which we started the section with. This is also analyzed using similar ideas. Towards that, we state the following lemma which can be proved using the Frobenius density theorem:

Lemma (Frobenius). *Let $h \in \mathbf{Z}[X]$ be monic, and assume that $h(X) \equiv 0 \bmod p$, has a solution in $\mathbf{Z}$ for almost all non-zero primes p. Then every element of the Galois group of $h(X)$ over Q fixes at least one root of h.*

Conversely, let h be monic and assume that every element of the Galois group of $h(X)$ over $\mathbf{Q}$ fixes at least one root of h. Then $h(X) \equiv 0 \pmod p$ has a solution in $\mathbf{Z}$ for every non-zero prime p.

To prove this lemma, let us recall the following weaker version of the Frobenius density theorem:

The set of primes p modulo which a monic integral, irreducible polynomial f has a given decomposition type $n_1, n_2, \ldots, n_r$, has density equal to $N/O(\mathrm{Gal}(f))$ where $N = |\{\sigma \in \mathrm{Gal}(f) : \sigma$ has a cycle pattern $n_1, n_2, \ldots, n_r\}|$.

Look at the first part. Assume that h is irreducible of degree > 1, if possible. The Frobenius Density Theorem shows that every σ has a cycle pattern of the form $1, n_2, \ldots$ This means that every element of $\mathrm{Gal}(h)$ fixes a root, say β. Since h is irreducible, the group $\mathrm{Gal}(h)$ acts transitively on the roots of h. Thus, this group would be the union of the conjugates of its subgroup H consisting of those elements which fix the root β. But a finite group cannot be the union of conjugates of a proper subgroup; this implies H is the whole group. Hence $\mathrm{Gal}(h)$ fixes each root of h and is therefore trivial. So we get h to be a linear polynomial, a contradiction.

The converse is proved as follows.

Let L be a splitting field of $h(X)$ over $\mathbf{Q}$. Let O_L be the ring of integers in L, and let P be a prime ideal of O_L lying over p. The roots of h lie in O_L by the assumption about h. Let D and I be the decomposition and inertia group of P respectively. Then D/I is cyclic, and maps isomorphically to the Galois group of the extension of residue fields.

Let $d \in D$ such that the coset dI generates D/I. By the assumption, d fixes a root z of h. Thus dI fixes the image of z in O_L/P. As dI generates the full Galois group of the residue field extensions, there is an integer b which is congruent to z modulo P. This gives $h(b) \in P \cap \mathbf{Z} = p\mathbf{Z}$, and the assertion follows.

Kronecker-conjugacy

We describe in outline some deep work of M. Fried ([4], [5], [6]) and later work by Peter Müller ([12]) relating to value sets of integer polynomials.

For $f \in \mathbf{Z}[X]$ and, p prime, consider the value set

$$\mathrm{Val}_p(f) = \{f(a) \mod p; a \in \mathbf{Z}\}.$$

Call $f, g \in \mathbf{Z}[X]$ to be *Kronecker-conjugate* if $\mathrm{Val}_p(f) = \mathrm{Val}_p(g)$ for all but finitely many primes p. In order to state a group-theoretic criterion for Kronecker-conjugacy, we need to fix some notations.

Given $f, g \in \mathbf{Z}[X]$ which are non-constant, consider a Galois extension K of the field $\mathbf{Q}(t)$ of rational functions in a variable t such that K contains a root x of $f(x) = t$ and a root y of $g(y) = t$. Let G denote $\mathrm{Gal}(K/\mathbf{Q}(t))$ and let U, V denote the stabilizers of x, y respectively.

Fried's Theorem.

Given $f, g \in \mathbf{Z}[X]$ which are non-constant, consider t, K, G, x, y, U, V as above. Then, f, g are Kronecker-conjugate if and only if

$$\bigcup_{g \in G} gUg^{-1} = \bigcup_{g \in G} gVg^{-1}.$$

Idea of Proof.

Suppose that f, g are Kronecker-conjugate. Write $f = uX^n + \cdots$ be of degree n. As Kronecker-conjugacy is preserved when we replace $f(X)$ and $g(X)$ by $u^{n-1}f(X/u)$ and $u^{n-1}g(X)$ respectively, we may assume that f is monic. Now, for any integer a, the hypothesis gives that $f(X) \equiv g(a) \pmod p$ has a root for almost all non-zero primes p. Hilbert's irreducibility theorem tells us that the Galois groups $\mathrm{Gal}(f(X) - g(y)$ over $K(y)$ and $\mathrm{Gal}(f(X) - g(a))$ over K are isomorphic as permutation groups for infinitely many a. Recall that $g(y) = t$. Thus every element of the Galois group $\mathrm{Gal}(f(X) - t)$ over $K(y)$ fixes at least one root. This Galois group is just the induced action of V on the roots of $f(X) - t$ (but V need not act faithfully). Hence every element in V fixes a root. But these roots are the conjugates of x whose stabilizer is U. So every element of V lies in some conjugate of U. By symmetry, the result follows.

Conjecture. *Over a field of characteristic* 0*, two polynomials f and g are Kronecker-conjugate if and only if, U and V are Gassmann equivalent; that is, the permutation representations* $\mathrm{Ind}_U^G \mathbf{1}$ *and* $\mathrm{Ind}_V^G \mathbf{1}$ *are equivalent.*

It should be noted that such a result is not purely group-theoretic because there are examples of abstract finite groups G and subgroups U, V such that $\bigcup_{g \in G} gUg^{-1} = \bigcup_{g \in G} gVg^{-1}$ but U, V are not Gassmann equivalent.

4. Dedekind's entirety conjecture

Dedekind conjectured that for number fields $K \subset L$, the ratio $\zeta_L(s)/\zeta_K(s)$ is an entire function of s. The Dedekind conjecture remains open in general. Actually, there is a more general conjecture due to Artin which we describe first. A proof of the Brauer-Aramata theorem appears in the classical text by J.-P. Serre [15] but we mention here a proof of Foote and Kumar Murty. The interested reader can also look at [14].

Let L/K be a Galois extension of number fields and let G denote the Galois group. For any prime ideal P of $\mathcal{O}_K$, look at the factorization $P\mathcal{O}_L = P_1^{e_1} \cdots P_g^{e_g}$. Now, the decomposition groups $D_{P_i} = \{\sigma \in G : \sigma(P_i) = P_i\}$ are mutually conjugate and the inertia subgroups $I_{P_i} = \{\sigma \in G : \sigma(x) \equiv x \mod P_i \ \forall\, x \in \mathcal{O}_L\}$ are the kernels of the natural surjections from D_{P_i} to Gal $((\mathcal{O}_L/P_i)/\mathcal{O}_K/P))$.

One also denotes by Fr_P, the Frobenius at P – this is a conjugacy class in G.

Artin associated to any finite-dimensional representation $\rho : G \to GL(V)$, an L-function defined as

$$L(s, \rho; L/K) = \prod_P det(1 - \rho(Fr_P)N_{K/Q}(P)^{-s}|V^{I_{P_i}})^{-1}.$$

Here $V^{I_{P_i}}$ is the subspace fixed by I_{P_i} for any i and the definition makes sense as Fr_P is a conjugacy class.

This Artin L-function has the following properties.

Properties:

(I) $L(s, \rho; L/K)$ depends only on the character χ_ρ and one often writes $L(s, \chi; L/K)$ for characters χ.

(II) If $\chi_1 \oplus \chi_2 = \chi$, then $L(s, \chi; L/K) = L(s, \chi_1; L/K)\, L(s, \chi_2; L/K)$.

(III) If H is a subgroup of G, then $L(s, \mathrm{Ind}_H^G(\chi); L/K) = L(s, \chi; L/L^H)$.

(IV) $L(s, \mathbf{1}; L/K) = \zeta_K(s)$.

(V) $L(s, \chi_{\mathrm{reg}}; L/K) = \zeta_L(s)$.

(VI) (Artin-Takagi factorization) $\zeta_L(s) = \prod_{\chi \in \hat{G}} L(s, \chi; L/K)^{\chi(1)}$.

Artin's Conjecture:

$L(s, \chi; L/K)$ extends to an entire function for any irreducible nontrivial character χ of G.

What Artin's reciprocity law means:

Artin's reciprocity law implies that Artin's conjecture holds for one-dimensional characters. More precisely:

If L/K is a Galois extension of number fields, and if χ is a monomial character of $\mathrm{Gal}(L/K)$ (that is, is induced from a one-dimensional character of some subgroup) and does not contain the trivial character, then $L(s, \chi; L/K)$ extends to an entire function of s.

Artin's conjecture implies Dedekind's entirety conjecture for $\zeta_L(s)/\zeta_K(s)$ in the case of Galois extensions L/K. However, without using Artin's conjecture, one can prove the above case of Dedekind conjecture – this is due to Brauer & Aramata.

Theorem (Brauer). *Let G be any finite group and χ an irreducible character of it. Then, there exist nilpotent subgroups $H_1, \ldots, H_r$ and one-dimensional characters ψ_i on H_i and integers n_i such that $\chi = \sum_{i=1}^r n_i \mathrm{Ind}_{H_i}^G(\psi_i)$.*

In fact, combined with Artin's reciprocity law, this theorem immediately implies the following one:

Theorem (Brauer). *Let L/K be a Galois extension of number fields. Let G denote the Galois group and let χ be an irreducible character of G. Then $L(s, \chi; L/K)$ admits a meromorphic continuation to the whole plane.*

Indeed, one need only observe that

$$L(s, \chi; L/K) = \prod_{i=1}^r L(s, \mathrm{Ind}_{H_i}^G(\psi_i); L/K)^{n_i}$$
$$= \prod_{i=1}^r L(s, \psi_i; L/L^{H_i})^{n_i}.$$

Heilbronn character

The behaviour of an Artin L-function at any point s_0 can be studied through the so-called *Heilbronn character*, a certain virtual character of $G = \mathrm{Gal}(L/K)$. If $n(G, \chi) := \mathrm{Ord}_{s=s_0} L(s, \chi; L/K)$, is the order of (zero/pole of) $L(s, \chi; L/K)$ at s_0 the Heilbronn character is:

$$\Theta_G(g) = \sum_\chi n(G, \chi)\chi(g).$$

The sum is over all irreducible characters of G. Notice that if Artin's conjecture is true, then this is an actual character when $s_0 = 1$. The following result was proved by Heilbronn:

Lemma. *For a subgroup H, the restriction of Θ_G to H is the Heilbronn character Θ_H of $\mathrm{Gal}(L/L^H)$.*

Proof. By the orthogonality of characters,

$$\Theta_G|H = \sum_{\chi \in \hat{G}} n(G, \chi) \left(\sum_{\psi \in \hat{H}} \langle \chi|H, \psi \rangle_H \psi \right)$$
$$= \sum_{\psi \in \hat{H}} \left(\sum_{\chi \in \hat{G}} n(G, \chi) \langle \chi, \mathrm{Ind}_H^G \psi \rangle_G \right) \psi$$

where the second equality follows from the Frobenius reciprocity theorem. Using the basic properties of the Artin L-function, we have

$$n(H, \psi) = \mathrm{Ord}_{s=s_0} L(s, \psi; L/L^H)$$
$$= \mathrm{Ord}_{s=s_0} L(s, \mathrm{Ind}_H^G \psi; L/K)$$
$$= \mathrm{Ord}_{s=s_0} \prod_\chi L(s, \chi; L/K)^{\langle \chi, \mathrm{Ind}_H^G \psi \rangle}$$
$$= \sum_\chi n(G, \chi) \langle \chi, \mathrm{Ind}_H^G \psi \rangle_G$$

which proves the lemma.

The following beautiful inequality was derived by R. Foote and V. Kumar Murty ([7]), and this has several consequences.

Lemma (Foote-Kumar Murty).

$$\sum_{\chi\in\hat{G}} n(G,\chi)^2 \le (\mathrm{Ord}_{s=s_0}\zeta_L(s))^2.$$

Proof. Now $\frac{1}{O(G)}\sum_{g\in G}|\Theta_G(g)|^2 = \langle\Theta_G,\Theta_G\rangle_G = \sum_{\chi\in\hat{G}} n(G,\chi)^2$.

We apply Heilbronn's lemma to the cyclic subgroups of G. We get

$$\Theta_G(g) = \Theta_{\langle g\rangle}(g) = \sum_{\psi\in\widehat{\langle g\rangle}} n(\langle g\rangle,\psi)\psi(g).$$

As the Artin reciprocity theorem implies that the Artin L-function is entire for one-dimensional characters, each $n(\langle g\rangle,\psi)\ge 0$. So $|\Theta_G(g)| \le \sum_{\psi\in\widehat{\langle g\rangle}} n(\langle g\rangle,\psi)$.

Finally, the Artin-Takagi factorization shows that

$$\mathrm{Ord}_{s=s_0}\zeta_L(s) = \sum_{\psi\in\widehat{\langle g\rangle}} n(\langle g\rangle,\psi)$$

for each element $g\in G$. Hence,

$$|\Theta_G(g)|^2 \le (\mathrm{Ord}_{s=s_0}\zeta_L(s))^2 \quad \forall \quad g\in G.$$

Corollary (Brauer-Aramata Theorem). *For any Galois extension L/K of number fields, the function $\zeta_L(s)/\zeta_K(s)$ is entire.*

Proof. Apply the Foote-Murty lemma and note that $\zeta_K(s) = L(s,\mathbf{1};L/K)$ where $\mathbf{1}$ is the trivial character of G.

Other variations have been obtained by M. Ram Murty and collaborators.

One such is:

Let $G = \mathrm{Gal}(L/K)$ with L/K, a solvable extension of number fields. Then

$$\sum_{1\ne\chi\in\hat{G}} n(G,\chi)^2 \le \left(\mathrm{Ord}_{s=s_0}\frac{\zeta_L(s)}{\zeta_K(s)}\right)^2$$

A group-theoretic lemma which they prove in this direction is:

Let G be a nontrivial finite, solvable group and H, a subgroup. Consider the derived series $\{G^{(i)}\}$ of G. Then, for all i,

$$\mathrm{Ind}_H^G\mathbf{1}_H = \mathrm{Ind}_{HG^{(i)}}\mathbf{1}_{HG^{(i)}} + \sum_j \mathrm{Ind}_{H_j}^G\theta_j$$

where θ_j's are 1-dimensional characters of some subgroups H_j which depend on H and i.

Using this lemma, A. Raghuram and M. Ram Murty prove:

Let $G = \mathrm{Gal}(L/K)$ with L/K, a solvable extension of number fields. Write L_{ab} denote the fixed field under $[G,G]$ and C denote the set of different 1-dimensional characters of G. Then

$$\sum_{1\ne\chi\in C} n(G,\chi)^2 \le \left(\mathrm{Ord}_{s=s_0}\frac{\zeta_L(s)}{\zeta_{L_{ab}}(s)}\right)^2$$

We end with a few smatterings of statements which occur in the Langlands program. First, we make a small observation to the effect that Artin's entirety conjecture needs to be proved only when the base is $\mathbf{Q}$. More precisely:

Artin cojecture enough to prove over Q:

Proposition. *If all nontrivial irreducible characters χ of $G := \mathrm{Gal}(E/\mathbf{Q})$ are so that $L(s,\chi,E/\mathbf{Q})$ extends to an entire function, then Artin's conjecture holds good.*

Proof. Let L/K be a Galois extension of number fields. Let E be the Galois closure over $\mathbf{Q}$ and let $G = \mathrm{Gal}(E/\mathbf{Q})$. Then $H = \mathrm{Gal}(L/K)$ is a subquotient of G. Let τ be any irreducible character of H and lift it to a character of $\mathrm{Gal}(E/K)$. Denote by θ the character of G induced from it. By Frobenius reciprocity law, θ does not contain the trivial character. In this case, by the property (II) we recalled earlier, $L(s,\theta,E/\mathbf{Q})$ is entire. But, the property (III) shows that $L(s,\theta,E/\mathbf{Q}) = L(s,\tau,L/K)$.

We end with the statement of one of the Langlands conjectures known as:

The Langlands reciprocity conjecture.

Let (V,ρ) be an n-dimensional irreducible representation of a Galois group $\mathrm{Gal}(L/K)$ of number fields. Then, there is a cuspidal automorphic representation π of $GL_n(\mathbf{A}_K)$ such that $L(s,\rho,L/K)$ is the L-function attached to π by Langlands.

We have not defined cuspidal automorphic representations or the corresponding L-function of Langlands but just remark that the latter L-functions are known to be entire!

References

[1] G. Andrews, The theory of partitions, Encyclopaedia of mathematics and its applications, Vol. 2, Addison-Wesley, Reading 176 (Reissued: Cambridge University Press 1985 and 1998).

[2] B. Berndt, Ramanujan's notebooks, Parts I–V, Springer, New York (1985, 1989, 1991, 1994, 1998).

[3] B.de Smit and H. W. Lenstra, Linearly equivalent actions of solvable groups, *J. of Algebra*, **228** (2000) 278–285.

[4] M. Fried, On a conjecture of Schur, *Michigan Math. J.*, **17** (1970) 41–55.

[5] M. Fried, The field of definition of function fields and a problem on the reducibility of polynomials in two variables, *Michigan Math. J.*, **17** (1973) 128–146.

[6] M. Fried, On Hilbert's irreducibility theorem, *J. of Numb. Theory*, *6* (1974) 211–231.

[7] R. Foote and V. Kumar Murty, Zeroes and poles of Artin L-series, *Math. Proc. Camb. Phil. Soc.*, **105** (1989) 5–11.

[8] F. Gassmann, Bemerkungen zu der vorstehenden Arbeit von Hurwitz, *Math. Z.*, **25** (1926), 124–143.

[9] I. M. Isaacs, Character theory of finite groups, Academic Press, New York (1976).

[10] B. Külshammer, J. B. Olsson and G. R. Robinson, *Generalized blocks for symmetric groups*, *Inventiones Mathematicae*, **151** (2003) 513–552.

[11] A. Maróti, On elementary lower bounds for the partition function, *Integers, Electronic Journal of Combinatorial Number Theory*, **3** (2003) #A10.

[12] P. Müller, Kronecker conjugacy of polynomials, *Trans. Amer. Math. Soc.*, **350** (1998) 1823–1850.

[13] R. Perlis, On the class numbers of arithmetically equivalent fields, *J. of Numb. Theory*, **10** (1978) 489–509.

[14] M. Ram Murty and A. Raghuram, Some variations on the Dedekind conjecture, *J. Ramanujan Math. Soc.*, **15** no. 4 (2000) 225—245.

[15] J.-P. Serre, Linear representations of finite groups, Springer-Verlag, GTM, **42** (1977).