Games with Galois

Daniel Mathews

July 30, 2007

1 Mathematics and Games

All the world's a stage, they say, and all the people merely players. Well, we might also say, all the world's a game, and all the people merely play them.

Mathematics is clearly home to a great many games and amusements. But the fruits of such excellent entertainment may extend to matters of even greater import than a closely-fought victory. There is no greater example than John Conway's celebrated *On Numbers and Games*, in which a full, rigorous development of numbers is presented starting from the concept of games. Conway produces the integers, rationals, infinitesimals, transfinite numbers and much more. So, occasionally games may be of use in other areas of mathematics, which are traditionally treated with more gravity: the present article is about another example.

Évariste Galois was no game theorist, but his infamous downfall arose from participation in an extraordinarily risky game — a duel with pistols at 25 paces. His tragic story is one of rejection, strife, passion and, as E. T. Bell put it, "massed stupidity aligned against him". His short but eventful life, swept up in the political currents of early nineteenth-century France, met with continual disaster. He was demoted at school; he was rejected from the esteemed Polytechnique twice (once, so the legend goes, putting the blackboard duster to better use as a missile against an imbecile examiner); his papers submitted to the Academy were lost, and on one occasion, the secretary responsible for his paper died; he was expelled from school for standing up for his democratic ideals; he joined the artillery of the National Guard to fight for the Republican cause; he was tried and acquitted for threatening the king; and then jailed simply for being "dangerous", later convicted on a trumped-up charge. The precise circumstances of his duel are not known: ostensibly it was over a woman, but it may also have involved his political rivals.

Today it is beyond doubt that Galois made epochal contributions to mathematics, despite his work being dismissed, neglected, or described as "incomprehensible" during his lifetime. By his death at the age of 20, young Évariste had established the branch of mathematics that today bears his name.

Galois theory is often regarded as a difficult area of mathematics. It's certainly not easy. But in a certain sense, as we shall see, it's all really just a game.

2 Solving as a learning game

The most immediately important question addressed by Galois theory is the solubility of polynomial equations. Our first player, valiantly attempting to solve polynomials, we will name Sol — she's very bright! The aim of any game, for her, is to solve polynomials.

Sol must convince me that a polynomial is soluble. While I understand algebra and general mathematical argument (sometimes), I am not very knowledgeable, and I only know the rational numbers. I want to be able to write down the solutions using the following symbols only:

$$+, -, \times, \div, \sqrt[n]{\cdot}$$

That is, Sol has to show me how to find the roots and write them as a radical expression.

Game 1. $x^2 + 1 = 0$. The roots, you should know, are $\pm i$. But I don't know that. How can Sol explain them to me? She could give me a lecture course about complex numbers, but that's asking a bit much. Rather, she could introduce a number α such that $\alpha^2 = -1$. Then the other root would be $-\alpha$. That is, she can introduce numbers *purely in terms of their algebraic properties.* Provided I am happy that, manipulating the end result by the rules, it satisfies the polynomial, that's not a problem. I can write the roots as $\pm\alpha$ or $\pm\sqrt{-1}$.

Here's an interesting question: is the number α supposed to be i or $-i$? Sol could again take the "complex numbers lecture course" approach, or think of other methods. But, if she sticks to purely algebraic properties of numbers, she *must fail*, because really i and $-i$ have identical algebraic properties: they both just sit there, until they're squared, at which point they become -1. Thus Sol's aim is an impossible one, and the numbers i and $-i$ are too symmetric for me to tell them apart. We must settle with simply writing down $\pm\alpha$ or $\pm\sqrt{-1}$ without really knowing what the individual numbers are in "reality". This may be a little disconcerting, but since I'm only worried about being able to write down roots as radical expressions, it's perfectly adequate.

In fact, for the same reasons, I can't ever distinguish between $\sqrt{5}$ and $-\sqrt{5}$, in fact any set of numbers satisfying the same irreducible rational polynomial. Such numbers are called *Galois conjugate.*

3 Symmetry strategy

Solving equations like the previous one really just amounts to taking square roots. Things get a bit more difficult when the polynomial is more complicated. Here we need to try something more interesting.

Let us first recall a few properties of polynomials. Consider a polynomial

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

and let the roots be $\alpha_1, \ldots, \alpha_n$. The roots allow us to factorise the polynomial:

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n).$$

Let's now assume our polynomial is *monic*, i.e. that the leading coefficient $a_n = 1$. We can equate our two descriptions of $p(x)$

$$x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n),$$

and then expanding out the brackets gives a rather complicated (but extremely useful!) equality.

$$\begin{aligned} x^n + a_{n-1}x^{n-1} + \cdots + a_0 &= x^n - (\alpha_1 + \cdots + \alpha_n)\, x^{n-1} + (\alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n)\, x^{n-1} \\ &\quad + \cdots + (-1)^n \alpha_1 \cdots \alpha_n \end{aligned}$$

Here, the expressions in brackets are very interesting. The coefficient of x^{n-1} is $-(\alpha_1 + \cdots + \cdots \alpha_n)$, the (negative) sum of the roots. The coefficient of x^{n-2}, written out a little more fully, is:

$$\begin{array}{ccccccccc} \alpha_1\alpha_2 & + & \alpha_1\alpha_3 & + & \alpha_1\alpha_4 & + & \cdots & + & \alpha_1\alpha_n \\ & + & \alpha_2\alpha_3 & + & \alpha_2\alpha_4 & + & \cdots & + & \alpha_2\alpha_n \\ & & & + & \alpha_3\alpha_4 & + & \cdots & + & \alpha_3\alpha_n \\ & & & & & + & \ddots & + & \vdots \\ & & & & & & & + & \alpha_{n-1}\alpha_n \end{array}$$

which is the *sum of all the possible products of two distinct roots*. It is itself a polynomial of the roots.

In general, a_{n-k} is (plus or minus) the *sum of all possible products of roots taken k at a time*. These expressions involving sums of all possible products of the roots are polynomials of the roots called *symmetric polynomials*. For instance, if $n = 3$, the symmetric polynomials are

$$\alpha_1 + \alpha_2 + \alpha_3, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \quad \alpha_1\alpha_2\alpha_3.$$

This gives us the following key fact; a nice relationship between the coefficients of a polynomial and the roots.

Fact 1. For a monic polynomial,

$$\begin{aligned} a_{n-1} &= -(\alpha_1 + \cdots + \alpha_n) \\ a_{n-k} &= (-1)^k \ \{ \text{ sum of all products of roots taken } k \text{ at a time } \} \\ a_0 &= (-1)^n \ \alpha_1\alpha_2\cdots\alpha_n \end{aligned}$$

Thus, the coefficients of a polynomial are (up to sign) the symmetric polynomials of the roots.

We will also take as a fact the following deeper theorem.

Fact 2. (Gauss' theorem on symmetric functions.) A polynomial in $\alpha_1, \cdots, \alpha_n$ which is symmetric in all the variables can be expressed in terms of the symmetric polynomials above, i.e. in terms of $a_0, a_1, \ldots, a_{n-1}$.

For instance, take $n = 3$, and take a random polynomial in $\alpha_1, \alpha_2, \alpha_3$ which is symmetric in all the variables, say $\alpha_1^3 + \alpha_2^3 + \alpha_3^3$. Then Gauss' theorem says that we can express this polynomial in terms of the standard symmetric polynomials,

namely $\alpha_1+\alpha_2+\alpha_3$, $\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3$ and $\alpha_1\alpha_2\alpha_3$. Indeed, if we look hard enough, we see that this is possible!

$$\begin{aligned}\alpha_1^3+\alpha_2^3+\alpha_3^3 &= (\alpha_1+\alpha_2+\alpha_3)^3 - 3(\alpha_1+\alpha_2+\alpha_3)(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)+3\alpha_1\alpha_2\alpha_3\\ &= -a_2^3+3a_1a_2-3a_0\end{aligned}$$

That took some effort, but Gauss' theorem tells us that if we seek long enough, we shall find!

With that background behind us, it's time for another game.

Game 2. $x^2-6x+7=0$. Let the roots be α,β. By the above formulae

$$\alpha+\beta=6, \qquad \alpha\beta=7.$$

S: Consider the expression $(\alpha-\beta)^2$. This is symmetric in α and β: if we swap them, we get $(\beta-\alpha)^2$ which is obviously the same.

D: Right! By Gauss' theorem, then, we can express it in terms of the symmetric polynomials $\alpha+\beta=6$ and $\alpha\beta=7$.

S: Precisely. We get

$$(\alpha-\beta)^2=(\alpha+\beta)^2-4\alpha\beta=6^2-4\times 7=8.$$

So I'm going to introduce to you this number $\sqrt{8}$, which has the property that its square is 8. If you play around with the algebra you'll see that the square of $\sqrt{8}/2$ is 2. So you can write it as $2\sqrt{2}$ if you like.

D: OK, I'm happy with that, I know algebra.

S: Now we've got $\alpha+\beta=6$ and $\alpha-\beta=2\sqrt{2}$. Solving the simultaneous equations easily gives

$$\alpha=3+\sqrt{2}, \quad \beta=3-\sqrt{2}$$

Using this method we can solve quadratics in general.

Game 3. x^3-2. (As you know, the roots are

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right), \quad \sqrt[3]{2}\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)$$

but I don't know that.)

S: Well, there's this number $\sqrt[3]{2}$, it's a number α described by the property that $\alpha^3=2$. I won't even bother to distinguish it from the other roots, because they're all Galois conjugates.

D: OK, great, $\alpha=\sqrt[3]{2}$ is a root. I now know the rational numbers and this number α. But what are the other two?

At this point, Sol can try to describe to me the other two roots by using rational numbers and α. But without introducing any new numbers, this is an impossible task. Using $\sqrt[3]{2}$ and rational numbers, she can't possibly describe complex numbers to me, only real ones. She must introduce a new number.

S: Well, there's this number $\sqrt[3]{2}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}\right)$. It's a number β so that $\beta^3-2=0$.

D: Hmmm... sounds like α.

S: Well it's one of the roots other than α.

D: That's a bit silly, why don't you factorise out $(x-\alpha)$ then?!

$$\begin{aligned} x^3-2 &= \left(x-\sqrt[3]{2}\right)\left(x^2+\sqrt[3]{2}x+\sqrt[3]{4}\right) \\ &= (x-\alpha)(x^2+\alpha x+\alpha^2) \end{aligned}$$

D: You should have said, "there's this number β that satisfies $\beta^2+\alpha\beta+\alpha^2=0$". It would have been more efficient. That's fine, I can solve the quadratic and obtain the two roots as

$$\alpha\left(\frac{-1+\sqrt{-3}}{2}\right), \qquad \alpha\left(\frac{-1-\sqrt{-3}}{2}\right).$$

4 Multi-stage learning and partial symmetry

As we just saw, with cubics I don't learn everything in one fell swoop. I need to learn in several stages. With a more difficult cubic, the problems become much worse. As we'll see, we need to consider equations which are only partially symmetric as we go.

Game 4. $x^3-6x-2=0$. Let the roots be α,β,γ so that

$$\alpha+\beta+\gamma=0, \quad \alpha\beta+\beta\gamma+\gamma\alpha=-6, \quad \alpha\beta\gamma=2.$$

S: First, there's this number ω, a cube root of unity. It satisfies $\omega^2+\omega+1=0$ and we'll write it as

$$\omega=\frac{-1+\sqrt{-3}}{2}.$$

D: Hmmm... yes, we can solve quadratic equations now. But I can't really see the point of this.

S: Give me a minute. Do you agree that ω is a cube root of unity, $\omega^3=1$?

D: Well, I know algebra, but all I know is that $\omega^2 + \omega + 1 = 0$. Let me see:

$$\begin{aligned} \omega^3 &= \omega^2 \cdot \omega \\ &= (-\omega - 1) \cdot \omega \\ &= -\omega^2 - \omega \\ &= 1. \end{aligned}$$

OK! I'm with you now.

S: Great. Introduce the two numbers y and z, which are defined in terms of the roots of the cubic.

$$y = \alpha + \omega\beta + \omega^2\gamma, \quad z = \alpha + \omega^2\beta + \omega\gamma.$$

D: I see, you're trying to find a symmetric function in α, β, γ, just like in the quadratic case. But hang on a minute, these aren't symmetric! If you swap α and β around, for instance, both the expressions for y and z change!

S: Yes, you're right. But if you *cycle* α, β, γ around in y, then y becomes $y\omega$ or $y\omega^2$... I'll show you.

$$\begin{aligned} \alpha\beta\gamma &\to \beta\gamma\alpha, \\ y = \alpha + \omega\beta + \omega^2\gamma &\to \beta + \omega\gamma + \omega^2\alpha \\ &= \omega^3\beta + \omega^4\gamma + \omega^2\alpha \\ &= \omega^2\left(\alpha + \omega\beta + \omega^2\gamma\right) \\ &= \omega^2 y \end{aligned}$$

Similarly z becomes ωz or $\omega^2 z$. So if we consider

$$y^3 = \left(\alpha + \omega\beta + \omega^2\gamma\right)^3, \quad z^3 = \left(\alpha + \omega^2\beta + \omega\gamma\right)^3$$

then both y^3 and z^3 are invariant under cycles.

D: That's tricky! You are very bright, Sol! But neither expression is symmetric!

S: Correct. But they are *partially* symmetric — if we content ourselves with only cycling α, β, γ around. On the other hand, if you do a swap like $\alpha \leftrightarrow \beta$ then you change y^3 into z^3!

$$\begin{aligned} \alpha\beta\gamma &\to \alpha\gamma\beta \\ y^3 = \left(\alpha + \omega\beta + \omega^2\gamma\right)^3 &\to \left(\beta + \omega\alpha + \omega^2\gamma\right)^3 \\ &= \left(\omega^3\beta + \omega\alpha + \omega^2\gamma\right)^3 \\ &= \omega^3\left(\alpha + \omega^2\beta + \omega\gamma\right)^3 = z^3 \end{aligned}$$

D: You're quite the algebra whiz!

S: Therefore, if we add y^3 and z^3 together, then they're invariant under any permutation! The same applies if we multiply them to get y^3z^3!

$$\begin{aligned} y^3+z^3 &= \left(\alpha+\omega\beta+\omega^2\gamma\right)^3+\left(\alpha+\omega^2\beta+\omega\gamma\right)^3, \\ y^3z^3 &= \left(\alpha+\omega\beta+\omega^2\gamma\right)^3\left(\alpha+\omega^2\beta+\omega\gamma\right)^3 \end{aligned}$$

D: That's very cool.

S: No, Galois is cool. Thus, y^3+z^3 and y^3z^3 are totally symmetric. By Gauss' theorem on symmetric functions, they can be written in terms of $\alpha+\beta+\gamma$, $\alpha\beta+\beta\gamma+\gamma\alpha$ and $\alpha\beta\gamma$ alone. In fact I did some algebra earlier and figured out that

$$\begin{aligned} y^3+z^3 &= 2\left(\alpha+\beta+\gamma\right)^3-9(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)+27\alpha\beta\gamma, \\ y^3z^3 &= \left(\alpha+\beta+\gamma\right)^6-9\left(\alpha+\beta+\gamma\right)^2(\alpha\beta+\beta\gamma+\gamma\alpha)^2-27(\alpha\beta+\beta\gamma+\gamma\alpha)^3. \end{aligned}$$

For our polynomial, we know that $\alpha+\beta+\gamma=0$, $\alpha\beta+\beta\gamma+\gamma\alpha=-6$, $\alpha\beta\gamma=2$. Therefore we have

$$y^3+z^3=54, \quad y^3z^3=18^3,$$

and y^3 and z^3 are the roots of the quadratic

$$t^2-54t+18^3=0.$$

D: We solved quadratics earlier. I'll solve this one.

$$y^3=27+27\sqrt{-7}, \qquad z^3=27-27\sqrt{-7}.$$

S: Now I'll teach you the number y, which satisfies the equation that its cube is y^3.

D: Der...!

S: Yes, but I had to teach you, otherwise you wouldn't know.

D: OK. I guess so.

$$y=\sqrt[3]{27+27\sqrt{-7}}=3\sqrt[3]{1+\sqrt{-7}}, \quad z=\sqrt[3]{27-27\sqrt{-7}}=3\sqrt[3]{1-\sqrt{-7}}$$

S: Now we're nearly done! Remember we had $y=\alpha+\omega\beta+\omega^2\gamma$ and $z=\alpha+\omega^2\beta+\omega\gamma$. Now we know that $\omega+\omega^2=-1$, so

$$y+z=2\alpha-\beta-\gamma$$

and hence

$$y+z+(\alpha+\beta+\gamma)=3\alpha.$$

We know y and z, and we know $\alpha + \beta + \gamma = 0$. Therefore

$$\alpha = \frac{y+z}{3} = \sqrt[3]{1+\sqrt{-7}} + \sqrt[3]{1-\sqrt{-7}}.$$

The other roots can be found out similarly. I don't have to teach you any new numbers.

5 Galois theory

We'll need to know something about permutations. Recall that a *permutation* of a set of objects is just a rearrangement of them. Speaking formally, a permutation is a bijective function from a set of objects to itself. Normally, if there are n objects, we just use the numbers $1, 2, \ldots, n$. We may write permutations in different ways:

$$12345 \to 23145, \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$
$$1 \mapsto 2 \mapsto 3 \mapsto 1, \quad 4 \mapsto 4, \quad 5 \mapsto 5$$
$$(123)(4)(5)$$
$$(123).$$

The last type of notation is called cycle notation and we say, for instance, that (123) is a *3-cycle*. In the last line, we used the common notational convenience of omitting 1-cycles like (4) and (5), since they just stay where they are. The way in which the cycles are grouped in a permutation is called its *cycle structure*. Thus (123)(45) and (124)(35) have the same cycle structure — they are $(2,3)$- or $(3,2)$-*cycles* — but (123)(45) and (123) do not. Permutations are multiplied by composing the functions involved. We multiply from left to right. For instance

$$(123)(45) \cdot (345) = (1243)(5) = (1243).$$

The do-nothing, or identity permutation is denoted (1). Permutations form a *group*: when you multiply two permutations, you get another permutation; each permutation has an *inverse* permutation which undoes it; and the multiplication is *associative*. Subsets of the set of permutations which have these properties are called *subgroups*.

Now it's worth summarising how we solved the cubic:

1. $y^3 + z^3$ and $y^3 z^3$ are rational. The expressions for them were totally symmetric. That is, they were invariant under *any* permutation of α, β, γ — the entire permutation group S_3.

$\alpha\beta\gamma$	$\alpha\gamma\beta$	$\beta\alpha\gamma$	$\beta\gamma\alpha$	$\gamma\alpha\beta$	$\gamma\beta\alpha$
(1)	(23)	(12)	(123)	(132)	(13)

2. Then we learnt y^3 and z^3 — an intermediate level of understanding — as the roots of a quadratic. y^3 and z^3 were not totally symmetric, but

they were invariant under cycles of α, β, γ. The expressions for them were *partially* symmetric — symmetric under cycling but not swaps. These cycles form a subgroup of S_3 called A_3.

$$\begin{array}{ccc} \alpha\beta\gamma & \beta\gamma\alpha & \gamma\alpha\beta \\ (1) & (123) & (132) \end{array}$$

3. Then we learnt y and z, by taking cube roots. They are the roots of a (really easy) cubic. The expressions for them are not symmetric at all! They were only invariant under the trivial permutation.

4. Understanding y and z is really the same level of understanding as α, β, γ, since we can then describe the roots in terms of y and z.

Galois' amazing idea is that stages of learning, and types of symmetry, are the same thing.

Theorem 5.1 (Fundamental theorem of Galois theory) *There is a one-to-one correspondence between levels of understanding in solving a general degree-n polynomial, and subgroups of the group of permutations of the n roots.*

This statement is necessarily imprecise, since we have not bothered to define anything properly. The correspondence is order-reversing.

Knowledge	$\mathbb{Q}$	$\subset$	$\mathbb{Q}, y^3, z^3$	$\subset$	$\mathbb{Q}, y, z \Rightarrow \alpha, \beta, \gamma$
Subgroup	S_3	$\supset$	A_3	$\supset$	(1)

Thus, the appropriate thing to do in solving polynomial equations is not to perform algebraic torture, but to find the appropriate middle levels of symmetry, and find expressions with that symmetry. With higher degree polynomials we need more levels of symmetry, because the middle levels of symmetry must be fairly "close together". If I am to be able to write down the answer as a radical expression, the only way to jump to a new level of understanding is when the "loss of symmetry" corresponds to "taking an n'th root".

The technical condition is that we must have a nested sequence of subgroups which have abelian quotients, down to the trivial group. A group which has such a sequence of subgroups is called *soluble*. The cubic polynomial is soluble precisely because the group S_3 is soluble. It turns out that solubility is equivalent to the derived series of the group eventually becoming trivial. I won't define these concepts here. Suffice it to note that the real game is about permutations; specifically, about whether or not sufficient "middle levels" of symmetry — that is, intermediate subgroups of permutations — exist.

6 The Game of Galois

Here is a game about permutations then. Since the actual game involved in determining whether a group is soluble is quite complicated, we'll start with a simpler version. Sol has a friend named Insol, who as the name suggests, insolently maintains that many polynomials are insoluble.

Definition 6.1 (n-Galois-lite) *Sol chooses a starting permutation x_0 of $\{1, 2, \ldots, n\}$, which cannot be the identity, and then takes no further part in the game. Insol chooses a permutation y_0, which* must have the same cycle structure as x_0. *We then form $x_0y_0 = x_1$. Insol chooses another permutation y_1 with the same cycle structure as x_1, and forms $x_1y_1 = x_2$. Play continues in this fashion. If Insol can keep away from the identity permutation for arbitrarily long, she wins. If she hits the identity, Sol wins.*

This sounds like a peculiar game. But the idea, in a more refined version of the game, is as follows: in a soluble group of permutations, Insol is forced to move down to lower levels of symmetry, eventually to the identity.

Game 5. $n = \infty$. We have ∞ objects, say the natural numbers $1, 2, \ldots$, but the players are only permitted to permute finitely many at a time.

Insol has a winning strategy in this game. Because there is an infinite set of objects, Insol can always pick a permutation which affects only objects which have been hitherto unused. When these permutations are multiplied, we just write the cycles next to each other! E.g.

$$(12)(34) \cdot (56)(78) = (12)(34)(56)(78).$$

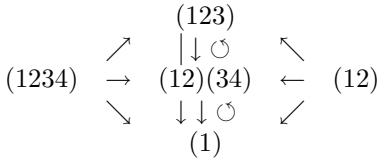
Game 6. $n = 1$. This is a non-starter, literally. There's only the identity permutation, so Sol cannot begin.

Game 7. $n = 2$. Sol can only choose (12) to start, and Insol can only respond with (12). Then $(12)(12) = (1)$ and Sol wins.

Game 8. $n = 3$. Sol has two types of permutations to use, either the (123) type or the (12) type. Hopefully you should be able to see that choosing different starting permutations with the same cycle structure makes no difference to the overall strategy.

Suppose Sol starts with (123). Then Insol responds with (123) and we form $(123)(123) = (132)$. Then Insol chooses (132) and we form $(132)(132) = (123)$. If Insol continues alternately choosing (123) and (132), she can keep away from the identity indefinitely and win. We'll call this the *copy* tactic. Sol must try something else, and starts with (12). But, alas, it is to no avail and Insol chooses (13), giving $(12)(13) = (123)$ and from there can maintain a 3-cycle with the copy tactic. Thus Insol has a winning strategy.

Game 9. $n = 4$. This is a little more complicated, but no matter how Sol starts, Insol can get to a permutation of the form (123) or (12)(34) and maintain it. The following diagram shows the possible moves Insol can make between the various cycle structures.



[figure 1]

For instance, if Sol starts with (1234) then Insol chooses (1342) and obtains $(1234)(1342) = (243)$, and can stay there by the copy tactic. If Sol starts with (12)(34) then Insol can stick there, choosing (13)(24) to get $(12)(34)(13)(24) = (14)(23)$, maintaining a $(2,2)$-cycle. So Insol wins again.

In general, Insol has many strategies available. First, Insol can remove any cycle she wants in a permutation, because each cycle has an inverse, which is obtained by writing it backwards. For example $(123)(321) = (1)$. The inverse has the same cycle structure, and Insol can choose it as part of her permutation. Second, the copy tactic can be applied to any odd-length cycle, so Insol can preserve an odd-length cycle. For instance, if (1234567) comes up, then Insol copies with (1234567) which gives $(1234567) \cdot (1234567) = (1357246)$. Third, a long even-length ($2k \geq 4$) cycle can be reduced to a $(2k-1)$-cycle, since, for instance, $(12345678) \cdot (21345678) = (2468357)$. Finally, a 2-cycle can be turned into a 3-cycle, as we saw previously. Combining all these tactics gives

Theorem 6.2 *Insol has a winning strategy in n-Galois-lite for any $n \geq 3$.*

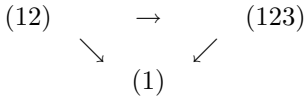
So much for the lite version of the game, which appears to be a bit easy for Insol! Let's toughen it up a bit.

Definition 6.3 (restricted n-Galois) *Again we have n objects and Sol selects a non-identity permutation x_0 to start. Again Insol selects a permutation y_0 with the same cycle structure as x_0. Then we set $x_0 y_0 x_0^{-1} y_0^{-1} = x_1$. Insol chooses y_1 with the same cycle structure as x_1, and we form $x_1 y_1 x_1^{-1} y_1^{-1} = x_2$. Play continues; if Insol can keep away from* (1) *indefinitely, she wins; otherwise Sol wins.*

Actually we can notice that axa^{-1} always has the same cycle structure as x, which is in turn the same as x^{-1}. The three permutations $y_n x_n^{-1} y_n^{-1}$, x_n^{-1} and x_n have the same cycle structure. In group theoretic language they are conjugates. If we allowed Insol to choose *any* permutation for y_n, the game would be identical to Galois-lite; hence the epithet "restricted".

Game 10. $n = 2$. Sol can only choose (12) to start and Insol can only choose (12) to obtain (1). Sol wins.

Game 11. $n = 3$. Sol can start with, say, (123) or (12). Suppose she chooses (123). Then Insol must choose (123) or (132), both of which yield (1), and Sol wins. On the other hand, if Sol starts with (12), then $y_0 x_0^{-1} y_0^{-1}$ will be a 2-cycle; the product of two 2-cycles is always of the form (abc) or (1). In any case, Sol wins.



Game 12. $n = 4$. Sol has 4 choices, namely (1234), (123), (12)(34), and (12). We can consider the following facts, gleaned from 4-Galois-lite.

The product of two 4-cycles is either of the form (abc), $(ab)(cd)$ or (1). This was illustrated for 4-Galois-lite above; in restricted Galois even fewer moves

are available. Similarly the product of two 2-cycles is either of the form (abc), $(ab)(cd)$ or (1). For similar reasons, once arriving at a cycle of the type (123), (12)(34) or (1), Insol cannot get back to a (1234) or (12).

Thus we only need consider permutations like (123), (12)(34) or (1). From (123), can Insol maintain a 3-cycle? The only way to do this is if $y_0(321)y_0^{-1} = (123)$, where y_0 is a 3-cycle. The 3-cycle cannot involve 4, and so must be (123) or (132). But the conjugate of (321) by both possibilities is again (321). So Insol cannot maintain a 3-cycle, and must go to a permutation of the form (12)(34) or (1). Similarly, Insol cannot maintain (12)(34): from (12)(34) all roads lead to (1).

Therefore, having considered all cases, we conclude that Insol fails, and Sol has a winning strategy for $n = 4$. There is a diagram of possible moves, which is the same as figure 1, with the loops removed.

7 The big game.

We now come to the final duel between Sol and Insol: the case $n = 5$. As we will see, it is on the outcome of this game that the fate of the solubility of the quintic polynomial turns.

Incidentally, the group S_5 of permutations on 5 elements is isomorphic to the group of isometries of a regular icosahedron. So this game can also be interpreted in terms of moving around (possibly reflecting at times) an icosahedron. Taking 3 pairs of opposite edges of an icosahedron appropriately, it is possible to form three mutually perpendicular golden rectangles. This can be done 5 different ways. The objects being permuted as the icosahedron is transformed are these 5 triads of rectangles. The relationship between the icosahedron and the quintic was explored by Felix Klein in [5].

Game 13. $n = 5$. Sol has a six-shooter, which can shoot (123)(45), or (12), or (1234), or (12345), or (12)(34), or (123).

First shot: Sol fires (123)(45). But Insol chooses (124)(35) to obtain (134) — a 3-cycle.

Second shot: Sol fires (12). But Insol deflects the shot with a (23), which results in (123).

Third shot: Sol fires (1234). Insol retaliates with (1243) to obtain (143).

Fourth shot: Sol fires (12345). But a quick (12354) ends with (254) and evades the blast.

Fifth shot: Sol fires (12)(34). Another conjugation from the hip, this time choosing (12)(35), gives (354).

Final shot: We may assume now that Insol is faced with an incoming 3-cycle, without loss of generality (123). But Insol now delivers the coup de gras, and chooses (145) to obtain (153). Insol has stabilised at a 3-cycle and is now invincible.

Theorem 7.1 *Insol wins the duel. That is, Insol has a winning strategy for restricted* 5*-Galois.*

The actual game involved in determining whether or not a general quintic polynomial is soluble is the following more complicated game. Play is identical to restricted n-Galois and n-Galois-lite, but the choices for Insol at each stage lie somewhere between the many choices of the lite version, and the fewer choices of the restricted version.

Definition 7.2 (n-Galois) *Sol chooses* $x_0 \neq (1)$*. Insol may select any permutation for* y_0*, then* $x_1 = x_0 y_0 x_0^{-1} y_0^{-1}$*. Call all the possible permutations for* x_1*, in any possible game,* level-1 *permutations. For* y_1*, Insol selects a level-1 permutation and we form* $x_2 = x_1 y_1 x_1^{-1} y_1^{-1}$*. The set of all possibilities for* x_2 *in any possible game are called* level-2 *permutations. Then* y_2 *must be a level-2 permutation, and so play continues. If Insol can avoid the identity, she wins; otherwise Sol wins.*

Those who know some group theory will see that the level-1 positions form S_n', the level-2 positions are S_n'', and so on; so Insol has a winning strategy if and only if S_n is insoluble.

However, because the n objects are indistinguishable, clearly all the permutations with the same cycle structure will be in the same levels. Therefore Insol has more moves than in restricted n-Galois, but less than in Galois-lite. So if Insol can win restricted n-Galois, she can win n-Galois.

Corollary 7.3 *Insol has a winning strategy for* 5*-Galois.*

Corollary 7.4 *The general quintic polynomial is insoluble by radicals.*

And, at last, the score is settled. The forces of insolubility win the day, at least for $n = 5$. I'll leave the other cases for you.

References

[1] E. T. Bell, Men of Mathematics (1937), 406–423

[2] John Conway, On Numbers and Games (1976)

[3] André Dalmas, Évariste Galois

[4] Évariste Galois, Oeuvres Mathématiques (1846)

[5] Felix Klein, Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree (1884) (English translation 1913 by G. G. Morrice)

[6] Ian Stewart, Galois Theory: Second Edition (1989)

— Daniel Mathews

Department of Mathematics, Stanford University, 94305 CA, USA
Email: mathews@math.stanford.edu
Web: http://math.stanford.edu/~mathews