Jordan Decomposition and Hensel's Lemma

One wants to study the action of T in on $\mathbb{Q}[T]/(P(T)^n)$ when $P(T)$ is an irreducible polynomial in $\mathbb{Q}[T]$.

How does one find such irreducible polynomials? Suppose $P(T)$ is a polynomial of the form $T^n + a_1T^{n-1} + \cdots + a_n$ where all the a_i are *integers*. Now, if p/q is a rational number that satisfies this polynomial then, by clearing denominators, we see that we have

$$p^n + a_1p^{n-1}q + \cdots + a_nq^n = 0$$

In that case, any prime factor of q also divides p^n and hence p. Thus, $p/q = b$ is an integer. In other words, we have shown that such a polynomial has a root in rationals if and only if it has an integer root.

If a polynomial has degree 2 or 3 and it can be factored, then at least one of the factors has degree 1. In other words, if it is *not* irreducible, then it has a linear factor. This can be combined with the above to show some polynomials are irreducible.

Exercise: Show that $T^2 + 1$ is irreducible.

Exercise: Show that $T^3 - T + 1$ is irreducible.

Gauss generalised the above to show that if $T^n + a_1T^{n-1} + \cdots + a_n$ is such that a_i are integers, then if it can be factored, then the factors too can be taken to have integer coefficients. This was used by Lagrange to give an explicit technique to determine if a polynomial is irreducible.

Repeated Roots

We have seen that if the minimal polynomial of a matrix has distinct roots over the complex numbers, then it is diagonalisable. Do we have a method to check whether a polynomial has distinct roots?

Let us define the *formal derivative* of a polynomial $P(T) = a_0T^n + a_1T^{n-1} + \cdots + a_n$ as

$$P'(T) = na_0T^{n-1} + (n-1)a_1T^{n-2} + \cdots + a_{n-1}$$

In other words, we have additivity $(P(T) + Q(T))' = P'(T) + Q'(T)$ and $(T^k)' = kT^{k-1}$.

Exercise: Check that the Liebnitz rule is satisfied:

$$(P(T) \cdot Q(T))' = P'(T)Q(T) + P(T)Q'(T)$$

Now, suppose that a polynomial $P(T)$ is written over complex numbers as $ P(T) = (T-z_1) \dots (T-z_n)$ where z_i are complex numbers which are not necessarily distinct.

Exercise: Check that the following identity holds:

$$P'(T) = \sum_{i=1}^{n} \frac{(T-z_1)\cdots(T-z_n)}{(T-z_i)}$$

Each term in the sum vanishes at z_i except possibly the i-th term. However, if $z_i = z_j$ for some $i \neq j$, then the i-th term vanishes as well since we get $z_i - z_j$ as a factor of the that term in $P'(z_i)$.

Thus, if $P(T)$ has repeated roots then $P(T)$ and $P'(T)$ have a common factor. In other words, if $P(T)$ and $P'(T)$ have no common factor, then the roots of $P(T)$ are distinct.

Exercise: (Starred) Show that the converse is also true. If $P(T)$ and $P'(T)$ have a common factor, then there is a repeated root.

In particular, we note that if $P(T)$ is irreducible in $\mathbb{Q}[T]$, then it cannot have a common factor with $P'(T)$ (which has smaller degree). Hence, it has distinct roots.

An Example

Let us consider the matrix A obtained as multiplication by T on $\mathbb{Q}[T]/(T^2+1)^2$. We wish to write $A = D + N$ where D is a diagonalizable matrix and N is a nilpotent matrix; we also want D and N to be expressed as polynomials in A.

Now, the element T in $\mathbb{Q}[T]/(T^2+1)$ already satisfies T^2+1 which has distinct roots over complex numbers. Any multiple of T^2+1 is nilpotent in $\mathbb{Q}[T]/(T^2+1)^2$. So we should look for $D = T - B(T)(T^2+1)$ so that $D^2+1 = 0$ in $\mathbb{Q}[T](T^2+1)^2$. Is this possible?

$$D^2+1 = (T-B(T)(T^2+1))^2+1 = T^2 - 2TB(T)(T^2+1) + B(T)^2(T^2+1)^2+1$$

Modulo $(T^2+1)^2$, this is $(T^2+1)(1-2TB(T))$. So, if we want this to be divisible by $(T^2+1)^2$, then we want $1-2TB(T)$ to be divisible by T^2+1. This can be arranged by taking $B(T) = -(1/2)T$.

In summary, we can take D to be the action of $T+(1/2)T(T^2+1)$ on $\mathbb{Q}[T]/(T^2+1)^2$. Then $D^2+1=0$ is the minimal polynomial of D and so D is diagonalisable over complex numbers. Moreover, $A-D$ is the action of $-(1/2)T(T^2+1)$ on this vector space and so it is nilpotent.

In order to generalise this we need to understand Hensel's Lemma (or the Newton-Raphson algorithm).

Another example

Before working out Hensel's Lemma in general, let us work out another example, in this case over integers.

We begin by noting that 2 is an element of $\mathbb{Z}/7$ such that $2^3 = 1$ in $\mathbb{Z}/7$. Can we find an element a in $\mathbb{Z}/7^3$ so that $a^3 = 1$ in that ring?

Let us start with an element of the form $2 + 7n$. We note that

$$(2 + 7n)^3 - 1 = 8 - 1 + 3 \cdot 2^2 \cdot (7n) \pmod{7^2} = 7(1 + 12n)$$

So we need to solve $1 + 12n = 0 \pmod 7$. We see easily that $n = 4$ is a solution to this. Thus, we see that $30 = 2 + 7 \cdot 4$ satisfies $30^3 = 1 \pmod{7^2}$. Next, we try something of the form $30 + 7^2 n$ to see if that has cube 1 modulo 7^3.

$$(30 + 7^2 n)^3 - 1 = 30^3 - 1 + 3 \cdot 30^2 \cdot (7^2 n) \pmod{7^3} = 7^2((30^3 - 1)/7^2 + 3 \cdot 30^2 n)$$

So we need to solve $(30^3 - 1)/7^2 + 330^2 n = 0 \pmod 7$. Now, $30 = 2 \pmod 7$ so this is the same a $(30^3 - 1)/7^2 + 12n = 0 \pmod 7$. As before, we can see that this can be solved by $n = 4 \cdot (30^3 - 1)/7^2$. Thus, we see that the solution we are looking for is $30 + 4 \cdot (30^3 - 1) \pmod{7^3} = 193$.

Hensel's Lemma

Is there a method to the above "madness"? The basic idea is as follows. Given a polynomial $P(T)$ such that $P(T)$ and $P'(T)$ have no common factor in $F[T]$ (for some field F). (As seen above, this is the same as the condition that no root is repeated.) We can then write $A(T)P(T) + B(T)P'(T) = 1$ for suitable polynomials $A(T)$ and $B(T)$.

Now consider the sequence of polynomials $A_n(T)$ defined inductively as follows $A_1(T) = T$.

$$A_{n+1}(T) = A_n(T) - B(T)P(A_n(T)) \text{ for } n \geq 1$$

We claim, by induction, that $P(A_n(T))$ is 0 in $F[T]/P(T)^n$. Suppose we have proved this upto some n (it is obvious for $n = 1$). To simplify notation, we write $A_{n+1}(T) = A_n(T) + E_n(T)$ and note that $E_n(T)$ is divisible by $P(T)^n$. Now we expand

$$P(A_{n+1}(T)) = P(A_n(T) + E_n(T)) = P(A_n(T)) + E_n(T)P'(A_n(T)) \pmod{P(T)^{n+1}}$$

since $E_n(T)^2$ and higher powers are divisible by $P(T)^{2n}$ and $2n \geq n+1$ since $n \geq 1$. Now substituting $E_n(T) = -B(T)P(A_n(T))$ we see that this becomes

$$P(A_{n+1}(T)) = P(A_n(T)) - B(T)P(A_n(T))P'(A_n(T)) = P(A_n(T))\,(1 - B(T)P'(A_n(T))$$

In order to make the right-hand side divisible by $P(T)^{n+1}$ we need to have $1 - B(T)P'(A_n(T))$ divisible by $P(T)$. Now, we see by construction that $A_n(T) = T \pmod{P(T)}$, so this becomes $1 - B(T)P'(T) \pmod{P(T)}$. By choice of $B(T)$ this is $A(T)P(T)$ and thus $0 \pmod{P(T)}$.

We note that by construction $T - A_n(T)$ is divisible by $P(T)$ and thus nilpotent in $F[T]/P(T)^n$. Hence we conclude that:

If $P(T)$ and $P'(T)$ have no common factor in $F[T]$, then the element T in $F[T]/P(T)^n$ can be written in the form $A_n(T) + N_n(T)$ where $P(A_n(T))$ is 0 in this ring and $N_n(T)$ is nilpotent in this ring.

This result is called the Jordan decomposition theorem since it allows us to decompose a matrix A which satisfies an equation of the form $P(T)^n$ where $P(T)$ and $P'(T)$ have no common factor into a form $A = D + N$ where D satisfies $P(D) = 0$ and N is nilpotent.