Notes for MA591U, Spring 2001
(Symbolic Computation)

Liouville's Theorem (Proof)

First, an overview of our approach. Let $\alpha \in \mathbb{F}$ and assume that $\int \alpha \in \mathbb{F}(t_1, \ldots, t_N)$, an elementary extension of $\mathbb{F}$. How can the t_i enter into an expression for $\int \alpha$ so that they disappear when one differentiates? We want to show that:

(i) $\left(\int \alpha = G(\ldots, \exp, \ldots)\right) \Rightarrow \left(\alpha = \cdots + \frac{\partial G}{\partial \exp} \cdot (\exp)' + \cdots\right)$ so no new $\exp$ can appear;

(ii) $\left(\int \alpha = G(\ldots, \ln x, \ldots)\right) \Rightarrow \left(\alpha = \cdots + \frac{\partial H}{\partial \ln x} \cdot \frac{\partial \ln x}{\partial x} + \cdots = \cdots + \frac{\partial H}{\partial \ln x} \cdot \frac{1}{x} + \cdots\right)$ so any new logs can appear only linearly in H, since they must disappear in $\frac{\partial H}{\partial \ln x}$;

(iii) there is no need for algebraics.

The point of the following lemma is that it allows us to describe expressions of the form u'/u and terms in partial fractions:

LEMMA: Let $\mathbb{F}$ be a differential field and $\mathbb{F}(t)$ a differential extension with no new constants. Assume t is not algebraic.

(i) If $t' \in \mathbb{F}$ and $f \in \mathbb{F}[t]$ such that $\deg f > 0$, then f' is a polynomial of the same degree as f, or one less, according to whether the highest coefficient of f is constant.

(ii) If $t'/t \in \mathbb{F}$, then for any $0 \neq a \in \mathbb{F}$ and $0 \neq n \in \mathbb{Z}$, $\exists 0 \neq h \in \mathbb{F}$ such that $(at^n)' = ht^n$. For any polynomial $f \in \mathbb{F}[t]$ of positive degree, f' is of the same degree, and is a multiple of f if, and only if, it is a monomial (i.e., $\exists n \in \mathbb{N}$ such that $f(t) = at^n$).

PROOF:

(i) Assume $t' = b \in \mathbb{F}$. Let $f(t) = a_n t^n + \cdots + a_0$ where $a_i \in \mathbb{F}$. Then

$$\begin{aligned} f'(t) &= \left(a_n' t^n + a_{n-1}' t^{n-1} + \cdots + a_1' t + a_0'\right) + \left(n a_n t' t^{n-1} + \cdots + a_1 t'\right) \\ &= a_n' t^n + (n a_n b + a_{n-1}' t) t^{n-1} + g(t) \end{aligned}$$

where g is of degree less than $n-1$. By way of contradiction, assume $\deg f' \leq n-2$, then $a_n' = 0$ and $n a_n b + a_{n-1}' = 0$. So

$$\left((n a_n t + a_{n-1})' = n a_n' t + n a_n t' + a_{n-1}' = 0 + n a_n b + a_{n-1}' = 0\right) \Rightarrow (n a_n t + a_{n-1} \in \mathbb{F})$$

(because $\mathbb{F}(t)$ introduces no new constants). But this contradicts the fact that t is not algebraic. Hence f' is a polynomial of the same degree as f, or one less, since $a_n' = 0$ if and only if $\deg f' = n-1$.

(ii) Assume that $b = t'/t \in \mathbb{F}$. Then for any monomial $at^n \in \mathbb{F}[t]$,

$$(at^n)' = a' t^n + a n t^{n-1} t' = (a' + anb) t^n.$$

So if $a' + anb = 0$, then $(at^n)' = 0$ and we have $at^n \in \mathbb{F}$, which contradicts the fact that t is not algebraic over $\mathbb{F}$. So $(at^n)' \neq 0$ and $\deg f' = \deg f$. If $f(t) = at^n$ – that is, if f is a monomial – we have just seen that there must be some $0 \neq h \in \mathbb{F}$ such that $f'(t) = ht^n$.

For the converse, suppose $f|f'$. This means $f' = \alpha f$ for some $\alpha \in \mathbb{F}$. By way of contradiction, suppose f has two terms $a_n t^n$ and $a_m t^m$. Then $(a_n t^n)' = \alpha a_n t^n$ and $(a_m t^m)' = \alpha a_m t^m$. Thus

$$\begin{aligned} \frac{(a_n t^n)'}{a_n t^n} &= \frac{(a_m t^m)'}{a_m t^m} \\ \frac{a_n' + n a_n b}{a_n} &= \frac{a_m' + a_m b}{a_m} \\ \frac{a_n'}{a_n} + n\frac{t'}{t} &= \frac{a_m'}{a_m} + m\frac{t'}{t} \end{aligned}$$

So

$$\begin{aligned} \frac{\left(\frac{a_n t^n}{a_m t^m}\right)'}{\frac{a_n t^n}{a_m t^m}} &= \frac{\frac{(a_n t^n)' \cdot a_m t^m - a_n t^n \cdot (a_m t^m)'}{(a_m t^m)^2}}{\frac{a_n t^n}{a_m t^m}} \\ &= \frac{\left(a_n' + n a_n b\right) a_m t^{m+n} - \left(a_m' + m a_m b\right) a_n t^{m+n}}{a_n t^n a_m t^m} \\ &= \frac{\left(a_n' + n a_n b\right) a_m t^{m+n}}{a_n a_m t^{m+n}} - \frac{\left(a_m' + m a_m b\right) a_n t^{m+n}}{a_n a_m t^{m+n}} \\ &= \frac{a_n' + n a_n n}{a_n} - \frac{a_m' + m a_m b}{a_m} \\ &= 0 \end{aligned}$$

and this implies that

$$\left[\left(\frac{a_n t^n}{a_m t^m}\right)' = 0\right] \Rightarrow \left(\frac{a_n t^n}{a_m t^m} \in \mathbb{F}\right)$$

which in turn implies that t is algebraic over $\mathbb{F}$. Again, we have a contradiction. Thus $f|f'$ implies that f has no more than one terms; that is, f is a monomial.

We have now shown that the lemma is true.

Next we need some Galois Theory. Let $\mathbb{Q} \subset \mathbb{F}$ and let $P \in \mathbb{F}[x]$. Some facts:

(1) $\exists \mathbb{F}(u_1, \ldots u_n) \supset \mathbb{F}$ with $P(u_i) = 0$ for each i.

(2) Given any two roots u_i and u_j, there is an automorphism $\sigma : \mathbb{F}(u_1, \ldots, u_n) \to \mathbb{F}(u_1, \ldots, u_n)$ with $\sigma(u_j) = u_j$.

(3) If all automorphisms σ with $\sigma|_{\mathrm{F}}$ fix $z \in \mathbb{F}(u_1, \ldots, u_n)$ then $z \in \mathbb{F}$.

(See Lang's *Algebra* for details of why these are true.)

LEMMA: Let $\mathbb{E}$ be a differential field, and assume it is an algebraic extension of some field $\mathbb{F}$. If σ is an automorphism of $\mathbb{E}$ and $\sigma(z') = \sigma(z)'$ for all $z \in \mathbb{F}$ then $\sigma(z') = \sigma(z)'$ for all $z \in \mathbb{E}$.

PROOF:

Define a new derivation D on $\mathbb{E}$ by $D(z) = \sigma^{-1}(\sigma(z)')$. (We omit the proof that this is a derivation.) Note that for $z \in \mathbb{F}$,

$$D(z) = \sigma^{-1}(\sigma(z)') = \sigma^{-1}(\sigma(z')) = z'.$$

This means that on $\mathbb{F}$, the derivations D and $'$ are the same. By the uniqueness of derivations, they must be the same on $\mathbb{E}$ as well, so $\sigma^{-1}(\sigma(z)') = z'$, which implies that $\sigma(z)' = \sigma(z')$.

Now we can prove Liouville's Theorem.

We have the elementary tower $\mathbb{F} \subset \mathbb{F}(t_1) \subset \cdots \subset \mathbb{F}(t_1, \ldots, t_N) = \mathbb{E}$. Let $y \in \mathbb{E}$ with $y' = \alpha \in \mathbb{F}$. We want to show that

$$\alpha = v' + \sum_i c_i \frac{u_i'}{u_i}$$

for $v, u_i \in \mathbb{F}$ and c_i constant in $\mathbb{F}$. We proceed by induction on N.

Applying the induction hypothesis, we can conclude that $\exists u_i, v \in \mathbb{F}(t_1)$ and c_i constant in $\mathbb{F}$ such that

$$\alpha = v' + \sum_i c_i \frac{u_i'}{u_i}.$$

Write t for t_1. We consider three cases.

Case 1: t is algebraic over $\mathbb{F}$.

Let P be the minimal polynomial of t over $\mathbb{F}$. Let $\mathbb{F}(w_1 = t_1, w_2, \ldots, w_m)$ be the field generated by the roots of P. Recall that the derivation on $\mathbb{F}$ extends uniquely to $\mathbb{F}(w_1, \ldots, w_m)$ and any automorphism that fixes $\mathbb{F}$ commutes with this derivation. Furthermore, any automorphism of $\mathbb{F}(w_1, \ldots, w_m)$ that fixes $\mathbb{F}$ is determined by its actions on the w_i. Hence, there are only a finite number of such automorphisms. Number them as $\sigma_1, \ldots, \sigma_s$. For each $j \in \{1, \ldots, s\}$ we have

$$\alpha = \sigma_j(\alpha) = \sigma_j\left(v' + \sum_i c_i \frac{u_i'}{u_i}\right) = \sigma_j(v)' + \sum_i c_i \frac{\sigma(u_i)'}{\sigma(u_i)}.$$

Then

$$\begin{aligned}\alpha &= \frac{1}{s}\left[\sum_j \sigma_j(v)' + \sum_i c_i \sum_j \frac{\sigma_j(u_i)'}{\sigma_j(u_i)}\right] \\ &= \frac{1}{s}\left[\left(\sum_j \sigma_j(v)\right)' + \sum_i c_i \frac{\left(\prod_j \sigma_j(u_i)\right)'}{\prod_j \sigma_j(u_i)}\right].\end{aligned}$$

Construct $V = \frac{1}{s}\sum_j \sigma_j(v)$ and $U_i = \prod_j \sigma_j(u_i)$. Then for any automorphism σ, we have $\sigma(V) = V$ and $\sigma(U_i) = U_i$. Hence $U_i, V \in \mathbb{F}$.

This tells us that we do not really need any new algebraics to integrate α.

For the remaining cases, we can assume that t is not algebraic. Let $\alpha \in \mathbb{F}$, $u_i, v \in \mathbb{F}(t)$ such that $\alpha' = v' + \sum_i c_i \frac{u_i'}{u_i}$. We can make some assumptions:

(i) We can write each u_i as a product $\prod_{i,j} u_{i,j}^{n_{i,j}}$ where each $n_{i,j} \in \mathbb{Z}$ and each $u_{i,j}$ is irreducible. So

$$\frac{u_i'}{u_i} = \sum_j n_{i,j} \frac{u_{i,j}'}{u_{i,j}}.$$

(ii) $\alpha = v' + \sum_i c_i \frac{u_i'}{u_i}$ where the u_i are monic, irreducible polynomials in t over $\mathbb{F}$.

(iii) v is the sum of polynomials and terms of the form q/f^r, where f is monic and irreducible.

Case 2: $(t = \ln(a)) \Rightarrow (t' = a'/a)$.

If f is monic and irreducible, then $\deg f' < \deg f$ (see the lemma from last time) so $f' \not| f$. Therefore $u_i = f$ implies that u_i'/u_i is in lowest terms.

If f appears in the partial fraction expansion of v – i.e., $v = \cdots + q/f^r + \cdots$, where r is the maximum exponent of f – then

$$v' = \cdots + \frac{q'}{f^r} - \frac{rqf'}{f^{r+1}} + \cdots.$$

Note that $f \not| rqf'$, so in the partial fraction decomposition of r', we have a term A/f^{r+1} with $r \geq 1$. Then

(i) f cannot appear in the denominator of v, since it could not cancel out in

$$v' + \sum_i c_i \frac{u_i'}{u_i} = \alpha \in \mathbb{F}$$

so $v \in \mathbb{F}[t]$;

(ii) f cannot be one of the u_i, because neither could it cancel then.

So $\alpha = v' + \sum_i c_i \frac{u_i'}{u_i}$ with $u_i \in \mathbb{F}$ and $v \in \mathbb{F}[t]$. But $v' \in \mathbb{F}$, so $v = ct + b$ (lemma) where c is a constant and $b \in \mathbb{F}$. Thus

$$\begin{aligned} \alpha &= (ct+b)' + \sum_i c_i \frac{u_i'}{u_i} \\ &= c\frac{a'}{a} + b' + \sum_i c_i \frac{u_i'}{u_i} \\ &= b' + c\frac{a'}{a} + \sum_i c_i \frac{u_i'}{u_i} \end{aligned}$$

with $a, b, u_i \in \mathbb{F}$, as desired.

Case 3: $\left(t = e^b\right) \Rightarrow (b = t'/t)$ for $b \in \mathbb{F}$.

What irreducible monic polynomials can occur in denominators? If f is a monomial, $f = t$. If f is not a monomial, $f \not| f'$ (by the lemma). So a similar argument as before shows that, if $f \neq t$, f cannot occur in a denominator. Hence

$$v = \sum_{i_0 \leq i \leq i_1} a_i t^i$$

and $u_i \in \mathbb{F}$, or at most one $u_i = t$. (In any case, $u_i'/u_i \in \mathbb{F}$.)

Hence $\alpha = v' + \sum_i c_i \frac{u_i'}{u_i}$. Since $\alpha \in \mathbb{F}$ and $\sum_i c_i \frac{u_i'}{u_i} \in \mathbb{F}$, $v' \in \mathbb{F}$. But $v' = \sum_i (a_i' + i a_i b') t^i$ and $a_i' + i a_i b' \neq 0$, so $i_0 = i_1 = 0$, and thus $v \in \mathbb{F}$. Hence α is of the desired form.