MATH 499: Notes

November 5, 2009

Starting with the integers \( \mathbb{Z} \), if we fix a positive integer \( n \), we can construct the integers modulo \( n \) as follows: we let

\[
\mathbb{Z}/\langle n \rangle = \{0, 1, 2, \ldots, n-1\}
\]

be the set of possible remainders upon dividing an integer by \( n \). To add or multiply \( x, y \in \mathbb{Z}/\langle n \rangle \), we add or multiply them in \( \mathbb{Z} \) and then take the remainder upon division by \( n \), e.g. we would write \( xy = qn + r \), and the product of \( x \) and \( y \) in \( \mathbb{Z}/\langle n \rangle \) would be \( r \).

If we replace \( \mathbb{Z} \) with a polynomial ring \( \mathbb{C}[x] \) in one variable, we can do more or less the same thing. Given a non-zero polynomial \( f \in \mathbb{C}[x] \) of degree \( n \), we define

\[
\mathbb{C}[x]/\langle f \rangle = \{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 : \ a_0, \ldots, a_{n-1} \in \mathbb{C}\}
\]

to again be the set of possible remainders upon division by \( f \). Again, for \( g, h \in \mathbb{C}[x]/\langle f \rangle \) we can define the sum or product of \( g \) and \( h \) to be the remainder upon division by \( f \) of their sum or product in \( \mathbb{C}[x] \).

With the help of Gröbner bases, we can do the same thing with polynomials in several variables. Fix a monomial order on \( \mathbb{C}[x_1, \ldots, x_k] \). Given an ideal \( I \subseteq \mathbb{C}[x_1, \ldots, x_k] \) we can find a Gröbner basis \( G \) for \( I \) and then define \( \mathbb{C}[x_1, \ldots, x_k]/I \) to be the set of possible possible remainders upon division by \( G \). But what are the possible remainders upon division by \( I \)?

---

1Alternatively, one says that \( x \) and \( y \) are congruent modulo \( n \) and write \( x \equiv y \pmod{n} \) if \( y - x \) is divisible by \( n \). One can check directly from the definition this relation satisfies the following properties (where \( \equiv \) denotes congruence modulo a fixed number \( n \)):

\[
\begin{align*}
    x & \equiv x \quad \text{for all } x \in \mathbb{Z} \\
    x \equiv y & \implies y \equiv x \quad \text{for all } x, y \in \mathbb{Z} \\
    x \equiv y \quad \text{and} \quad y \equiv z & \implies x \equiv z \quad \text{for all } x, y, z \in \mathbb{Z} \\
    x_1 \equiv x_2 \quad \text{and} \quad y_1 \equiv y_2 & \implies x_1 + y_1 \equiv x_2 + y_2 \quad \text{for all } x_1, y_1, x_2, y_2 \in \mathbb{Z} \\
    x_1 \equiv x_2 \quad \text{and} \quad y_1 \equiv y_2 & \implies x_1y_1 \equiv x_2y_2 \quad \text{for all } x_1, y_1, x_2, y_2 \in \mathbb{Z}
\end{align*}
\]

Properties 1-3 above show that congruence modulo \( n \) is an equivalence relation on \( \mathbb{Z} \), which thus partitions the set \( \mathbb{Z} \) into equivalence classes

\[
C_x = \{a \in \mathbb{Z} : \ a \equiv x \pmod{n}\}.
\]

We can then define

\[
\mathbb{Z}/\langle n \rangle = \{C_x : x \in \mathbb{Z}\}
\]

to be the set of equivalence classes, and define addition and multiplication on \( \mathbb{Z}/\langle n \rangle \) by setting \( C_x + C_y = C_{x+y} \) and \( C_x \cdot C_y = C_{xy} \); this is well-defined by properties 4 and 5 above. This is equivalent to the definition in terms of remainders: \( \mathbb{Z}/\langle n \rangle \) has \( n \) elements \( C_0, C_1, \ldots, C_{n-1} \) corresponding to the \( n \) possible remainders upon division by \( n \) and the addition and multiplication operations correspond to those defined above.

This definition has one advantage over the definition in terms of remainders: it generalizes (with no need for Gröbner bases) to the case where we replace \( \mathbb{Z} \) with \( \mathbb{Q}[x_1, \ldots, x_k] \) (or in fact any ring) and replace \( \langle n \rangle \) with any ideal \( I \). We define \( f \equiv g \pmod{I} \) to mean that \( g - f \in I \). Then we can again show that properties 1-5 above hold for this relation, and we set

\[
\mathbb{Q}[x_1, \ldots, x_k]/I = \{C_f : \ f \in \mathbb{Q}[x_1, \ldots, x_k]\}
\]

with addition and multiplication defined in the same way.
The possible remainders are those polynomials none of whose terms is divisible by a leading term of a polynomial in \( G \), or in other words the finite sums \( \sum \alpha a_\alpha x^\alpha \) where each \( x^\alpha \not\in \langle \text{LT}(I) \rangle \). It may then be the case that there are infinitely many monomials \( x^\alpha \) which are not in \( I \): for example, we may take \( I = \langle x^2y, xy^2 \rangle \subset C[x, y] \). Then the monomials that may appear in a remainder upon division by \( I \) are \( x^n \) and \( y^n \) for all \( n \geq 0 \), and the monomial \( xy^2 \). In this case \( C[x, y]/I \) is an infinite-dimensional vector space over \( C \), with basis the infinite set \{ \( x^\alpha : x^\alpha \not\in \langle \text{LT}(I) \rangle \) \}.

It is also possible that there are only finitely many monomials \( x^{\alpha_1}, \ldots, x^{\alpha_n} \) not in \( \text{LT}(I) \), so that

\[
C[x_1, \ldots, x_k]/I = \left\{ \sum_{i=1}^{n} a_\alpha x^{\alpha_i} \right\}
\]

is an \( n \) dimensional vector space over \( C \). For example, consider the ideal

\[
I = \langle x^2 + 2y^2 - 3, x^2 + xy + y^2 - 3 \rangle \subset C[x, y].
\]

We saw on the homework that in lex order, \( G = \{x^2 + 2y^2 - 3, xy - y^2, y^3 - y\} \) is a Gröbner basis for \( I \). There are thus exactly 4 monomials not in \( \langle \text{LT}(I) \rangle \), namely 1, \( x \), \( y \), and \( y^2 \). If \( X = V(I) \)

\begin{figure}[h]
\centering
\begin{subfigure}{0.49\textwidth}
\includegraphics[width=\textwidth]{a.png}
\caption{graphs of the curves}
\end{subfigure} \hspace{1cm}
\begin{subfigure}{0.49\textwidth}
\includegraphics[width=\textwidth]{b.png}
\caption{\( \langle \text{LT}(I) \rangle \) in lex order}
\end{subfigure}
\caption{The curves \( x^2 + 2y^2 = 3 \) and \( x^2 + xy + y^2 = 3 \)}
\end{figure}

is the set of four points where the polynomials of \( I \) all vanish, then we can think of \( C[x, y]/I \) as being the polynomial functions on \( X \). In our construction of \( C[x, y]/I \) we’re making functions \( f \) and \( g \) on the whole plane equivalent if they have the same remainder upon division by \( I \), i.e. if \( f = g + h \) where \( h \) is in \( I \) and thus is identically zero on \( X \). Thus in this example, the space of functions on the four points of \( X \) is four-dimensional, and so is \( C[x, y]/I \).

The dimension of \( C[x, y]/I \) isn’t always equal to the number of points in \( X = V(I) \) though. For example, consider the ideal

\[
J = \langle x^2 + 4y^2 - 4, 4x^2 - 8x + y^2 \rangle \subset C[x, y].
\]

Here, \( \{8x+15y^2-16, 225y^4-224y^2\} \) is a Gröbner basis for \( J \) in lex order, and \( Y = V(J) \) contains only 3 points, but there are 4 monomials not in \( \langle \text{LT}(J) \rangle \), namely 1, \( y, y^2 \), and \( y^3 \). Nor is this a

\footnote{The term order used to find the Gröbner basis for \( I \) doesn’t matter here because \( I \) itself is a monomial ideal}
peculiarity of lex order: if we use graded lex instead, we find that \{15y^2 + 8x - 16, 15x^2 - 32x + 4\} is a Gröbner basis and that \{1, x, y, xy\} is a vector space basis for \(\mathbb{C}[x, y]/J\), which still has dimension 4 as a vector space over \(\mathbb{C}\). This reflects the fact that while the curves \(x^2 + 4y^2 = 4\) and \(4x^2 - 8x + y^2 = 0\) only intersect in 3 points, their intersection at (1, 0) has “multiplicity 2” because the two curves are tangent there.

The Tjurina number of a plane curve singularity

Suppose \(C = V(f)\), with \(f \in \mathbb{C}[x, y]\) is a plane curve with a single singular point \(p\). We consider the Tjurina ideal

\[
I_f = \langle f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \rangle
\]

and set \(T_f = \mathbb{C}[x, y]/I_f\) and define the Tjurina number \(\tau(f)\) to be the dimension of \(T_f\) as a vector space over \(\mathbb{C}\), or in other words, the number of monomials not in \(\langle LT(I_f) \rangle\) for a fixed monomial order on \(\mathbb{C}[x, y]\). Since \(p\) is the only singular point of \(C\), it is also the only common zero of \(f\), \(\frac{\partial f}{\partial x}\), and \(\frac{\partial f}{\partial y}\).

It turns out that, like the multiplicity of the singularity, the Tjurina number \(\tau(f)\) is an invariant (e.g. if \(f\) is affine equivalent to \(g\), then \(\tau(f) = \tau(g)\)). Also, it is a new invariant: the Tjurina number is not simply a function of the multiplicity.

\[\text{3}\]

More generally, the particular monomials not in \(\langle LT(J) \rangle\) may depend on the monomial order, but the dimension of \(\mathbb{C}[x, y]/J\) as a \(\mathbb{C}\)-vector space (i.e. the number of such monomials) does not. This is because \(\mathbb{C}[x, y]/J\) can be defined abstractly in terms of congruence classes modulo \(J\), and this agrees with the construction of \(\mathbb{C}[x, y]/J\) using each monomial order.

\[\text{4}\]

We’ve only defined the intersection multiplicity of a curve and a line. For more information on the intersection multiplicity of two curves at a point in general, see section 8.7 of Cox, Little, and O’Shea, where it is defined using resultants.