Mathematics 466 **Proving theorems from Geometry** A. Hulpke

Suppose we describe points in the plane by their (x, y)-coordinates. We then can describe many geometric properties by polynomial equations:

Theorem: Suppose that $A = (x_a, y_a)$, $B = (x_b, y_b)$, $C = (x_c, y_c)$ and $D = (x_d, y_d)$ are points in the plane. Then the following geometric properties are described by polynomial equations:

$\overline{AB}$ **is parallel to** $\overline{CD}$**:** $\frac{y_b - y_a}{x_b - x_a} = \frac{y_d - y_c}{x_d - x_c}$, which implies $(y_b - y_a)(x_d - x_c) = (y_d - y_c)(x_b - x_a)$.

$\overline{AB} \perp \overline{CD}$**:** $(x_b - x_a)(x_d - x_c) + (y_b - y_a)(y_d - y_c) = 0$.

$|AB| = |CD|$**:** $(x_b - x_a)^2 + (y_b - y_a)^2 = (x_d - x_c)^2 + (y_d - y_c)^2$.

C **lies on the circle with center** A **though the point** B**:** $|AC| = |AB|$.

C **is the midpoint of** $\overline{AB}$**:** $x_c = \frac{1}{2}(x_b - x_a)$, $y_c = \frac{1}{2}(y_b = y_a)$.

C **is collinear with** $\overline{AB}$**:** self

$\overline{BD}$ **bisects** $\angle ABC$**:** self

A typical theorem in geometry now sets up as prerequisites certain points (and their relation with circles and lines) and claims (the conclusion) that this setup implies other conditions. If we label the coordinates of the points involved as (x_i, y_i) , then the prerequisites are described by a set of polynomials $f_j \in \mathbb{R}[x_1, \ldots, x_n, y_1, \ldots, y_n] =: R$. A conclusion similarly corresponds to a polynomials $g \in R$.

The statement of the theorem thus can be translated as follows: Whenever $\{(x_i, y_i)\}$ are points fulfilling the prerequisites (i.e. $f_j(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0$), then $g(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0$, that is the conclusion holds for these points.

Let $I = (f_1, \ldots, f_r) \lhd R$ the ideal generated by the prerequisite polynomials. Clearly *any* polynomial $h \in I$ will satisfy $h(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0$. However there might be other polynomials with the same roots that lie outside I. For example consider $I = \langle x^2 \rangle \lhd \mathbb{R}[x]$, then $g(x) = x \notin I$, but has the same roots.

An important theorem (which typically would be proven in graduate classes in commutative algebra or algebraic geometry) now shows that over $\mathbb{C}$, such a power condition is all that can happen[1]:

> **Theorem (Hilbert's Nullstellensatz):** Let $R = \mathbb{C}[x_1, \ldots, x_n]$ and $I \lhd R$. If $g \in R$ such that $g(x_1, \ldots, x_n) = 0$ if and only if $f(x_1, \ldots, x_n) = 0$ for all $f \in I$, then there exists an integer m, such that $g^m \in I$.

The set $\{g \in R \mid \exists m : g^m \in I\}$ is called the *Radical* of I.
(Caveat: Typically want real coordinates. Thus there is some extra subtlety in practice.)

There is a neat way how one can test this property, without having to try out possible m: Suppose that $I = \langle f_1, \ldots, f_m \rangle \lhd R$ and let $g \in R$. Then there exists a natural number m such that $g^m \in I$ if and only if (we introduce an auxiliary variable y)

$$1 \in \langle f_1, \ldots, f_m, 1 - yg \rangle =: \tilde{I} \lhd k[x_1, \ldots, x_n, y]$$

[1] Actually, one does not need $\mathbb{C}$, but only that the field is *algebraically closed*

The reason is easy: If $1 \in \tilde{I}$, we can write

$$1 = \sum_i p(x_1, \ldots, x_n, y) \cdot f_i(x_1, \ldots, x_n) + q(x_1, \ldots, x_n, y) \cdot (1 - yg)$$

We now set $y = 1/g$ (formally in the fraction field) and multiply with a sufficient high power (exponent m) of g, to clean out all g in the denominators. We obtain

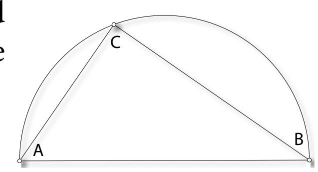
$$g^m = \sum_i \underbrace{g^m \cdot p(x_1, \ldots, x_n, 1/g^m)}_{\in R} \cdot f_i(x_1, \ldots, x_n) + \underbrace{g^m \cdot q(x_1, \ldots, x_n, y) \cdot (1 - y/y)}_{=0} \in I.$$

Vice versa, if $g^m \in I$, then

$$1 = y^m g^m + (1 - y^m g^m) = \underbrace{y^m g^m}_{\in I \subset \tilde{I}} + \underbrace{(1 - yg)}_{\in \tilde{I}}(1 + yg + \cdots + y^{m-1} g^{m-1}) \in \tilde{I}$$

There are computational methods for testing ideal membership, using a technique called *Gröbner bases*.

Thales' theorem For example, consider the theorem of Thales: Any triangle suspended under a half-circle has a right angle.
We assume (after rotation and scaling) that $A = (-1, 0)$ and $B = (1, 0)$ and set $C = (x, y)$ with variable coordinates. The fact that C is on the circle (whose origin is $(0, 0)$ and radius is 1) is specified by the polynomial



$$f = x^2 + y^2 - 1 = 0$$

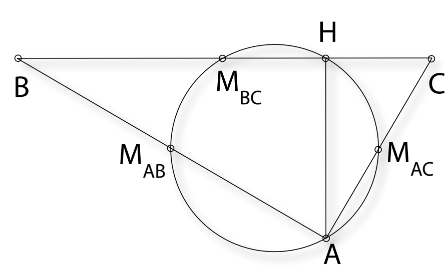
The right angle at C means that $\overline{AC} \perp \overline{BC}$. We encode this as

$$g = (x - (-1)) + (1 - x) + y(-y) = -x^2 - y^2 + 1 = 0.$$

Clearly g is implied by f.

Apollonius' theorem We want to use this approach to prove a classical geometrical theorem (it is a special case of the "Nine point" or "Feuerbach circle" theorem):

Circle Theorem of Apollonius: Suppose that ABC is a right angled triangle with right angle at A. The midpoints of the three sides, and the foot of the altitude drawn from A onto $\overline{BC}$ all lie on a circle.



To translate this theorem into equations, we choose coordinates for the points A, B, C. For simplicity we set (translation) $A = (0,0)$ and $B = (b,0)$ and $C = (0,c)$, where b and c are constants. (That is, the calculation takes place in a polynomial ring not over the rationals, but over the quotient field of $\mathbb{Q}[b,c]$.) Suppose that $M_{AB} = (x_1, 0)$, $M_{AC} = (0, x_2)$ and $M_{BC} = (x_3, x_4)$. We get the equations

$$\begin{aligned} f_1 &= 2x_1 - b = 0 \\ f_2 &= 2x_2 - c = 0 \\ f_3 &= 2x_3 - b = 0 \\ f_4 &= 2x_4 - c = 0 \end{aligned}$$

Next assume that $H = (x_5, x_6)$. Then $AH \perp BC$ yields

$$f_5 = x_5 b - x_6 c = 0$$

Because H lies on BC, we get

$$f_6 = x_5 c + x_6 b - bc = 0$$

To describe the circle, assume that the middle point is $O = (x_7, x_8)$. The circle property then means that $|M_{AB}O| = |M_{BC}O| = |M_{AC}O|$ which gives the conditions

$$\begin{aligned} f_7 &= (x_1 - x_7)^2 + (0 - x_8)^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0 \\ f_8 &= (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \end{aligned}$$

The conclusion is that $|HO| = |M_{AB}O|$, which translates to

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0.$$

We now want to show that there is an m, such that $g^m \in \langle f_1, \ldots, f_8 \rangle$. In GAP, we first define a ring for the two constants, and assign the constants. We also define variables *over* this ring.

```
R:=PolynomialRing(Rationals,["b","c"]);
ind:=IndeterminatesOfPolynomialRing(R);b:=ind[1];c:=ind[2];
x1:=X(R,"x1"); ... x8:=X(R,"x8");
```

We define the ideal generators f_i as well as g:

```
f1:=2*x1-b;
f2:=2*x2-c;
f3:=2*x3-b;
f4:=2*x4-c;
f5:=x5*b-x6*c;
f6:=x5*c+x6*b-b*c;
f7:=(x1-x7)^2+(0-x8)^2-(x3-x7)^2-(x4-x8)^2;
f8:=(x1-x7)^2+x8^2-x7^2-(x8-x2)^2;
g:=(x5-x7)^2+(x6-x8)^2-(x1-x7)^2-x8^2;
```

For the test whether $g^m \in I$, we test that 1 is in the ideal $\tilde{I} = (f_1, \ldots, f_8, 1 - yg) \lhd R[y]$, using a Gröbner basis for $\tilde{I}$:

```
order:=MonomialLexOrdering();
bas:=ReducedGroebnerBasis([f1,f2,f3,f4,f5,f6,f7,f8,1-y*g],order);
```

The basis returned is (1), which means that indeed $g^m \in I$.
If we wanted to know for which m, we can test membership in I itself, and find that already $g \in I$:

```
gap> bas:=ReducedGroebnerBasis([f1,f2,f3,f4,f5,f6,f7,f8],order);
[ x8-1/4*c, x7-1/4*b, x6+(-b^2*c/(b^2+c^2)), x5+(-b*c^2/(b^2+c^2)),
  x4-1/2*c, x3-1/2*b, x2-1/2*c, x1-1/2*b ]
gap> PolynomialReducedRemainder(g,bas,order);
0
```