Thm Every ideal I in $R = k[x_1, \dots x_n]$ has a unique reduced Gröbner basis.

Scetch of proof

- Start with any G.B., turn into a reduced G.B.
- Divide each $g \in G$ by it leading coefficient

want to remove all elements g in G whose initial monomial is not a minimal generator of $in_c(I)$.

- For any pair $g, g' \in G$ if $in_c(g) = in_c(g')$ discard one of g, g'
- For $g \in G$ use division alg. to comput the remainder r of g divided by G and replace g by r ∎

Computing GB

Thm (Divison Algorithm). Work in $R = K_c[x_1, \dots, x_n]$. Let $\{f_1, \dots, f_s\}$ be an ordered list of polynomials in R

Every $f \in R$ can be written as

$$f = q_1 f_1 + \dots + q_s f_s + \underbrace{r}_{\text{remainder}}$$

where $q_i, r \in R$ s.t.

$r = 0$ OR r is a K-linear combo of monomials, none of when are divisible by any of $in_c(f_1), \dots, in_c(f_s)$

Further if $q_i f_i \neq 0 \Rightarrow in_>(f) \geq in_>(q_i f_i)$

Ideal membership

It is clear if $r=0$ above

$\Rightarrow f = q_1 f_1 + \dots + q_s f_s \Rightarrow f \in I = \langle f_1, \dots, f_s \rangle$

However for an arbitary gen. set this ($r=0$ after division) only suffcient, but not nessary for $f \in I$.

Ex) Let $f_1 = xy-1$, $f_2 = y^2-1$ in $k_{lex}[x,y]$

Divide $f = xy^2 - x$ by $\{f_1, f_2\}$ gives

$$xy^2 - x = \underbrace{y}_{q_1} \cdot (xy-1) + \underbrace{0}_{q_2} \cdot (y^2-1) + (\underbrace{-x+y}_{r})$$

Divide f by $\{f_2, f_1\}$ gives

$$xy^2 - x = x(y^2-1) + 0 \cdot (xy-1) + 0$$

we will see that if G is G. B., in any mon. order, the division algorithm answers if $f \in \langle G \rangle$.

Prop) Let $I \subseteq R = k[x_1, \dots, x_n]$, $G = \{g_1, \dots, g_t\}$ be a Gröbner basis of I. Given $f \in R$ there exists a unique $r \in R$ s.t.

1) No term of r is divisable by any of $in_<(g_1), \dots, in_<(g_t)$

2) There is $g \in I$ s.t. $f = g + r$

In particular r is the remainder after division by G no matter order the elements of G are listed in.

Proof: By the division Alg an r satisfying 1), 2) exists.

Prove uniqueness:

Suppose $f = g + r = g' + r'$ satisfying 1), 2)

$\Rightarrow \quad r - r' = g' - g \in I$

Since G.B.

If $r \neq r' \Rightarrow \quad in_<(r-r') \in in_<(I) = \langle in_<(g_1), \dots, in_<(g_t) \rangle$

$\Rightarrow \quad in_<(g_i) \mid in_<(r-r')$ for some g_i

But, by div alg, no term of r, r' is divisible

by any of $in_<(g_1), \dots, in(g_t)$

$\therefore \quad in_<(g_i) \nmid in_<(r-r')$

since terms must be some monomial in r or r'

Cor Let $G = \{g_1, \dots, g_t\}$ be a G.B. for $I \subseteq K[x_1, \dots, x_n]$ an ideal, and $f \in K[x_1, \dots, x_n]$. We have $f \in I$ iff the remainder on division of f by G is zero.

Def (LCM) Let $f, g \in K_<[x_1, \dots, x_n]$ be non-zero and suppose that $in_<(f) = x^a$, $in_<(g) = x^b$

then $x^\gamma = lcm(in_<(f), in_<(g))$, where $\gamma = \max(a_i, b_i)$

Def (Lead term). $f \in K_<[x_1, \dots, x_n]$ with $f = LC \cdot in_<(f) + \text{lower terms}$, $LC \in K$

$LT(f) = LC \cdot in_<(f)$.

Def (S-poly) The S-polynomial of $f, g \neq 0$ in $K[x_1,\dots,x_n]$

is
$$S(f,g) = \operatorname{lcm}(\operatorname{in}(f), \operatorname{in}(g)) \cdot \left(\frac{f}{LT(f)} - \frac{g}{LT(g)} \right)$$

This "designed" to cancel lead terms

Def Given a set $G = \{g_1,\dots,g_r\}$ and a poly f (all in $K[x_1,\dots,x_n]$)

write $f \% G$ or $\operatorname{rem}(f, G)$ for the remainder of dividing f by G.

Lemma $f, g \in K_<[x_1,\dots,x_n]$ non-zero. Then
$\operatorname{in}_<(S(f,g)) < \operatorname{lcm}(\operatorname{in}_<(f), \operatorname{in}_<(g))$.

Lemma * Suppose we have $\sum_{i=1}^{s} p_i$ where $p_i \in K[x_1,\dots,x_n]$ $\operatorname{in}_<(p_i) = x^\delta \ \forall i$

If $\operatorname{in}_<\left(\sum p_i\right) < x^\delta$ then $\sum p_i$ is a K-linear combo of $S(p_i, p_j)$

Further $\operatorname{in}_<(S(p_i, p_j)) < x^\delta \quad \forall i,j$.

Lemma ** Let $c_a, c_b \in K$, $g_a, g_b \in K[x_1,\dots,x_n]$ non-zero,

suppose $\operatorname{in}_<\left(S(c_a x^a \cdot g_a, c_b x^b \cdot g_b) \right) = x^\delta$. Then

we have
$$S(x^a g_a, x^b g_b) = x^{\delta - \gamma} S(g_a, g_b)$$

where $x^\gamma = \operatorname{lcm}(\operatorname{in}_<(g_a), \operatorname{in}_<(g_b))$.

Thm (Buchberger Criterion). Let $I \subseteq K_<[x_1,\dots,x_n]$ be an ideal.

Then $G = \{g_1,\dots,g_t\}$, where $I = \langle g_1,\dots,g_t \rangle$, is a Gröbner basis for I iff for all pairs $i \neq j$ the remainder $S(g_i, g_j) \% G = 0$.

Proof | $\Rightarrow$

If G is a G.B. then, since $S(g_i, g_j) \in I$ the remainder on div by G is zero.

$\Leftarrow$ Now suppose $S(g_i, g_j) \% G = 0 \quad \forall i \neq j$

Let $f \in I$, non-zero, show that $in_<(f) \in \langle in_<(g_1), \dots, in_<(g_t) \rangle$

Write $f = \sum_{i=1}^{t} h_i g_i$, $h_i \in k[x_1, \dots, x_n]$

Note that

$$in_<(f) \leq \max(in_<(h_i g_i))$$

Among all expressions $f = \sum h_i g_i$ pick one

s.t. $x^\delta = \max(in_<(h_i g_i))$ is minimal

$\therefore \quad in_<(f) \leq x^\delta$

If $in_<(f) = in_<(h_i g_i)$ for some i

$$\Rightarrow \quad in_<(g_i) \mid in_<(f)$$

$$\therefore \quad in_<(f) \in \langle in_<(g_1), \dots, in_<(g_t) \rangle.$$

Suppose $in_<(f) < x^\delta$

goal: use fact $S(g_i, g_j) \% G = 0 \; \forall i \neq j$ to contradict minimality of x^δ.

$$f = \sum_{in_<(h_i g_i) = x^\delta} h_i g_i + \sum_{in_<(h_i g_i) < x^\delta} h_i g_i$$

$$= \sum_{in(h_i g_i) = x^\delta} \overbrace{LT(h_i) g_i}^{\sim\sim\sim\; -\; (*)} + \sum_{in(h_i g_i) = x^\delta} (h_i - LT(h_i)) g_i + \sum_{in(h_i g_i) < x^\delta} h_i g_i$$

Let $w = \sum LT(h_i) g_i$
$in(h_i g_i) = x^\delta$

$in_<$ are $< x^\delta$

But $in_<(f) < x^\delta$ by assumption

$\therefore in_<(w) < x^\delta$

By Lemma * w is a k-linear combination of S-polys $S(LT(h_i)g_i, LT(h_j)g_j) = x^{\delta - \gamma_{ij}} S(g_i, g_j)$

↑ by Lemma **

where $x^{\gamma_{ij}} = lcm(in_<(g_i), in_<(g_j))$

$\therefore$ w is a K-lin combo of $x^{\delta-\gamma_{ij}} S(g_i, g_j)$,

and by assumption $S(g_i, g_j) \% G = 0$

$\therefore$ By division Alg

$$S(g_i, g_j) = \sum A_\ell g_\ell \quad ; A_\ell \in K[x_1, \dots, x_n]$$

and $in_<(A_\ell g_\ell) \le in_<(S(g_i, g_j))$ when $A_\ell g_\ell \ne 0$

So $x^{\delta-\gamma_{ij}} S(g_i, g_j) = \sum \underbrace{x^{\delta-\gamma_{ij}} A_\ell}_{B_\ell} g_\ell$

Then by $in_<(B_\ell g_\ell) \le in_<(x^{\delta-\gamma_{ij}} S(g_i, g_j)) < x^\delta$

↑ By Lemma ‡

since $in_<(S(g_i, g_j)) < lcm(in_<(g_i), in_<(g_j)) = x^{\gamma_{ij}}$

w is a K-linear combo of $B_\ell g_\ell$

and $in_<(B_\ell g_\ell) < x^\delta$

$\therefore$ f is a k-linear combo of terms $< x^\delta$ which contradicts minimality of x^δ. $\blacksquare$

Thm (Ascending Chain Condition) Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be an ascending chain of ideals in $k[x_1, \dots, x_n]$

Then $\exists$ an $N \geq 1$ s.t

$$I_N = I_{N+1} = I_{N+1} = \cdots$$

Proof Set $I = \bigcup_{i=1}^{\infty} I_i$ (check that this is an ideal)

By the Hilbert basis thm $I = \langle f_1, \dots, f_s \rangle$

but each $f_i \in I_{j_i}$ for some j_i $\forall i$

$$N = \max(j_1, \dots, j_s)$$

$\Rightarrow$ $f_i \in I_N$ $\forall i$ since we an ascending chain

$\therefore$ $I = \langle f_1, \dots, f_s \rangle \subseteq I_N \subseteq \cdots \subseteq I$

$\Rightarrow$ $I_N = I_{N+1} = I$. $\blacksquare$

Thm (Buchberger's Algorithm) Let $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$ in $k[x_1, \dots, x_n]$. Then a Gröbner basis for I can be computed in a finite number of steps by the following algorithm

Algorithm:

Input: $F = \{f_1, \dots, f_s\}$

Output: a Gröbner basis $G = (g_1, \dots, g_t)$ for I with $F \subseteq G$.

Procedure:

```
G := F
Repeat := true

While Repeat DO:
    G' := G
    For each pair {p,q}, p≠q, in G' DO:
        r := S(p,q) % G'
        IF r≠0 Then G := G ∪ {r}

    IF G == G' Then (Repeat := false; Return G;)
```

Proof Show $G \subseteq I$ at every step

$G = F$ is okay

when we enlarge G we add $S(p,q) \% G$, $p, q \in I$

$\Rightarrow S(p,q) \in I$

$\Rightarrow S(p,q) \% G \in I$

$\therefore G \cup \{r\} \in I$.

and G contains $f_1, \dots, f_s \Rightarrow I \subseteq \langle G \rangle$ and $G \subseteq I$

$\therefore I = \langle G \rangle$

The alg. stops when $G = G'$ at all steps

meaning $S(p,q) \% G' = 0 \quad \forall\, p, q$

$\therefore$ G is a G.B. by Buchberger's Criterion.

End of Lecture

Rest of proof:

We must show the Alg terminates, want to use the Ascending chain condition

At each step G consists of G' (=old G) together with non-zero remainders of S-polynomials of pairs in G', i.e.

initial monomials of all polys in G'

$$\langle in_<(G') \rangle \subseteq \langle in_<(G) \rangle$$

Note that if $G' \neq G \Rightarrow \langle in_<(G') \rangle \overset{\text{strict}}{\subsetneq} \langle in_<(G) \rangle$

Since if $r = S(p,q) \% G' \neq 0 \quad (p, q \in G')$

$$\Rightarrow \quad in_<(g') \nmid in_<(r) \quad \forall g \in G'$$

$$\therefore \quad in_<(r) \notin \langle in_<(G') \rangle \text{ but}$$

$$in_<(r) \in \langle in_<(G) \rangle$$

If we write $G', G'', \ldots, G^{(n)}, \ldots$ etc for the "G" appearing in the loop. we have an Ascending chain

$$\langle in_<(G') \rangle \subseteq \langle in_<(G'') \rangle \subseteq \cdots$$

$\therefore$ by ACC

$$\langle in_<(G^{(n)}) \rangle = \langle in_<(G^{(n+1)}) \rangle \quad \text{for some } n$$

$$\Rightarrow \quad G^{(n)} = G^{(n+1)} = G$$ (otherwise we must have proper containment of the monomial ideals)

$\therefore$ The algorithm terminates ∎