A11.1 Homogeneous polynomials

Definition A11.1.1. A homogeneous polynomial in $n$ variables of degree $d$ is an element of the span of the monomials of degree $d$. A monomial of degree $d$ has the form $x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ with $\sum_{i=1}^n e_i = d$. Let $H_d(n)$ denote the space of homogeneous polynomials in $n$ variables of degree $d$.

Note that if a polynomial is homogeneous of degree $d$ then for any scalar $\lambda \in F$ we have $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_1, \ldots, x_n)$.

Exercise A11.1.2. Assume the field $F$ is infinite. Prove: if a polynomial $f \in F[x]$ satisfies $f(\lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_1, \ldots, x_n)$ for every scalar $\lambda \in F$ then $f$ is homogeneous of degree $d$.

Example A11.1.3. The following polynomial is homogeneous of degree 3:

$$x_1^2x_3 + 4x_1x_4x_5 + 7x_2^3.$$ 

Let us compute the dimension of $H_d(n)$. First note that $H_1(n)$ is spanned by $x_1, \ldots, x_n$ and therefore $\dim H_1(n) = n$. The basis of $H_2(n)$ can be split into two groups $x_i^2$ and $x_ix_j$ ($i \neq j$). This shows that $\dim H_2(n) = n + \binom{n}{2} = \binom{n+1}{2}$. Next, we compute $\dim H_3(n)$ by splitting the monomials of degree 3 into three groups.

$$H_3(n) = \text{Span}(\{x_i^3\} \cup \{x_i^2x_j\}_{i \neq j} \cup \{x_ix_jx_k\}_{i < j < k}).$$

Clearly, the first and third sets contribute $n + \binom{n}{3}$ elements. The second set contributes $n(n-1)$ elements since the roles of $i$ and $j$ are not symmetric, so we have $n$ choices for the square and then $n-1$ choices for the non-square. Now we get, by brute calculation,

$$\dim H_3(n) = n + n(n-1) + \binom{n}{3} = \binom{n+2}{3}.$$

Exercise A11.1.4. Prove that $\dim H_d(n) = \binom{n+d-1}{d}$. Hint: Count monomials by giving a bijection to a set which is easier to count directly.
A11.2 Euclid’s algorithm

Definition A11.2.1. Suppose that \( f \) and \( g \) are elements of a commutative ring with identity (e.g. the integers, or univariate polynomials over a field). Then \( f \mid g \) if there exists \( h \) such that \( g = fh \).

Homework: study Euclid’s gcd algorithm for integers, using, e.g., web resources (MathWorld, Wikipedia, etc.). The algorithm is based on the

Theorem A11.2.2. ("Division Theorem") Given integers \( a, b \) such that \( b \neq 0 \), there exists integers \( q, r \) such that \( a = qb + r \) and \( 0 \leq r < |b| \).

Polynomials also have a Euclidean algorithm. Our convention is that \( \text{deg} \ 0 = -\infty \).

Theorem A11.2.3. (Division Theorem for polynomials) For any polynomials \( f(x) \) and \( g(x) \neq 0 \) over a field, there exist polynomials \( q(x) \) and \( r(x) \) over the same field such that \( f(x) = q(x)g(x) + r(x) \) where \( \text{deg} r(x) < \text{deg} f(x) \).

Definition A11.2.4. (Greatest common divisors) Let \( a, b \) be either integers or univariate polynomials over a field. Then \( d \) is a greatest common divisor of \( a \) and \( b \), if

(i) \( d \mid a \) and \( d \mid b \), and

(ii) whenever \( d' \) divides both \( a \) and \( b \) it must be the case that \( d' \mid d \).

Note that this is a wish-list; there is no a priori guarantee that a number or polynomial satisfying these requirements exists.

Moreover, the gcd, if exists, is not unique. Among the integers, if \( d \) is a greatest common divisor of \( a, b \) then so is \( -d \). These are the only two in the case of the integers. We reserve the notation \( \gcd(a, b) \) for the positive greatest common divisor.

If \( a \) and \( b \) are polynomials then their gcd is unique up the nonzero scalar multiples (if \( x^2 + 3 \) is a gcd then so is \( 7x^2 + 21 \)).

Exercise A11.2.5. (a) Prove that the gcd of polynomials over a filed is unique up to nonzero scalars. (b) What is the situation over \( \mathbb{Z}[x] \)?

Homework A11.2.6. Study Euclid’s algorithm. Prove that a greatest common divisor (satisfying our definition) exists for integers or polynomials.

How can we determine whether two polynomials have a common factor, or even their greatest common divisor? One method is to use the Euclidean algorithm. Observe that if \( a \) and \( b \) are integers, then \( \gcd(a, b) \) divides every integer linear combination of \( a \) and \( b \). In fact, by iterating the Euclidean algorithm, we can arrive at an expression \( \gcd(a, b) = xa + yb \) for some integers \( x, y \).

Example A11.2.7. Given integers \( a = 28, b = 231 \), write \( 231 = 8 \times 28 + 7 \) so we already have \( 7 = 231 + (-8) \times 28 \). Typically, more steps are needed to find a linear combination expressing the gcd.
Exercise A11.2.8. Let \( k, l > 0 \) and prove that
\[
\gcd(a^k - 1, a^l - 1) = a^{\gcd(k,l)} - 1.
\]

Exercise A11.2.9. Show that a greatest common divisor over \( \mathbb{Q}[x] \) is a greatest common divisor over \( \mathbb{C}[x] \).

A11.3 Greatest common divisor as a linear combination

Theorem A11.3.1. If \( H \leq (\mathbb{Z},+) \) then \( H \) is cyclic, i.e. there exists \( d \in \mathbb{Z} \) such that \( H = d\mathbb{Z} := \{dn : n \in \mathbb{Z}\} \).

Proof. If \( H = \{0\} \) then we take \( d = 0 \). Assume that there exists \( 0 \neq a \in H \). Then \( a - a = 0 \in H \) and \( 0 - a = -a \in H \). Furthermore if \( a, b \in H \) then \( -b \in H \) so \( a - (-b) = a + b \in H \).

Even more, if \( k \in \mathbb{N} \) then \( ka = a + \cdots (k \text{ times}) + a \in H \) and \( (-k)a = -(ak) \in H \). So \( H \) is closed under taking integer-linear combinations of elements. In \( d\mathbb{Z} \), \( d \) is the smallest positive number. Therefore we should consider the smallest positive number in \( H \). Let \( d = \min\{x \in H : x > 0\} \) (there are positive numbers in \( H \) since there is a nonzero number \( x \in H \) and one of \( x, -x \) is positive).

Claim A11.3.2. \( H = d\mathbb{Z} \).

Indeed, consider \( 0 \neq h \in H \). We may assume that \( h > 0 \) (by replacing \( h \) with \( -h \) if need be). Write \( h = qd + r \) where \( 0 \leq r < d \). Note that \( -qd \in H \) so \( h - qd = r \in H \). But \( d \) is the smallest positive number and therefore \( r = 0 \). So \( d \mid h \). Similarly \( d \mid -h \). Of course it is now clear that \( H = d\mathbb{Z} \).

Here is an application of this theorem. If \( a, b \in \mathbb{Z} \) consider the set \( H = \{xa + yb : x, y \in \mathbb{Z}\} \subset \mathbb{Z} \). Observe that this set is a subgroup of \( \mathbb{Z} \) since it is evidently nonempty and closed under subtraction. By the theorem \( H = d\mathbb{Z} \). Note \( a, b \in H \) so \( d \mid a, b \). Furthermore \( d = xa + yb \) for some choice of \( x, y \in \mathbb{Z} \). So if \( d' \mid a, b \) then \( d' \mid xa + yb = d \). Hence \( d \) is a greatest common divisor of \( a \) and \( b \)!

Corollary A11.3.3. Given two integers \( a \) and \( b \), a greatest common divisor of \( a \) and \( b \) exists and can be expressed as an integer linear combination of \( a \) and \( b \).

Exercise A11.3.4. If \( x, y \in \mathbb{Z} \) are such that \( xa + yb \) is a common divisor of \( a \) and \( b \) then \( xa + yb \) is a greatest common divisor.

Exercise A11.3.5. Let \( a, b \neq 0 \) be integers. There are \( x, y \) such that \( |x| < |b| \) and \( |y| < |a| \) such that \( xa + by = \gcd(a, b) \).

Exercise A11.3.6. Let \( F_n \) be the \( n^{th} \) Fibonacci number. Then \( \gcd(F_k, F_l) = F_d \) where \( d = \gcd(k, l) \). (Recall that \( F_0 = 0, F_1 = 1, \) and \( F_n = F_{n-1} + F_{n-2} \).)
A11.4 Greatest common divisor of polynomials

You will see in the next bunch of exercises that there is a very similar story when we replace the integers with polynomials in one variable over a field.

Definition A11.4.1. Let $H \subset F[x]$. $H$ is an ideal of $F[x]$ (denoted $H \triangleleft F[x]$) if it is nonempty, closed under subtraction, and for any $h(x) \in H$ and $f(x) \in F[x]$ we have $f(x)h(x) \in H$.

Clearly, if $d(x) \in F[x]$ is a polynomial then the set $d(x)F[x] := \{d(x)f(x) : f(x) \in F[x]\}$ is an ideal in $F[x]$. An ideal of the form $d(x)F[x]$ is called a principal ideal. In fact, these are the only ideals in $F[x]$:

Exercise A11.4.2. Prove that all ideals in $F[x]$ are principal. In other words, given an ideal $H \triangleleft F[x]$, prove that there exists $d(x) \in F[x]$ such that $H = d(x)F[x]$.

(Hint: follow the ideas of the proof of Theorem A11.3.1; use the “Division Theorem for polynomials.”)

Exercise A11.4.3. For every pair of polynomials $f(x), g(x)$ there exists a greatest common divisor $d(x) \in F[x]$ for $f$ and $g$ and $d(x) = u(x)f(x) + v(x)g(x)$ for some polynomials $u, v \in F[x]$.

Exercise A11.4.4. If $f, g \neq 0$ then we can choose $u, v$ as above to satisfy $\deg u < \deg g$ and $\deg v < \deg f$.

Exercise A11.4.5. If $f$ and $g$ are relatively prime then there exist unique polynomials $u, v$ such that $uf + vg = 1$ and $\deg u < \deg g$ and $\deg v < \deg f$.

A11.5 The resultant

We try to understand when two rational polynomials have a common complex root. While Euclid’s algorithm provides a way to decide this question, it does not give an explicit formula.

Sylvester showed that for $f, g \in F[x]$, there is a quantity $R(f, g)$ calculated by a determinant such that

$$R(f, g) = \begin{cases} 0 & \gcd(f, g) \neq 1, \\ \neq 0 & \gcd(f, g) = 1. \end{cases}$$

We shall find Sylvester’s determinant. Given

$f(x) = a_0 + a_1 x + \cdots + a_k x^k \quad a_k \neq 0$

$g(x) = b_0 + b_1 x + \cdots + b_l x^l \quad b_l \neq 0$

we are looking for

$u(x) = r_0 + r_1 x + \cdots + r_l x^{l-1}$

$v(x) = s_0 + s_1 x + \cdots + s_k x^{k-1}$
such that
\[ u(x)f(x) + v(x)g(x) = 1. \] (1)

There is a solution (a choice of \( r_i, s_j, k + l \) unknowns) if and only if \( \gcd(f, g) = 1 \).

The equation (1) provides a linear system of equations in \( r_i, s_j \). Calculate a little:

\[
\begin{align*}
u(x)f(x) &= a_0 r_0 + (a_0 r_1 + a_1 r_0)x + \cdots + a_k r_{l-1} x^{k+l-1} \\
v(x)g(x) &= b_0 s_0 + (b_0 s_1 + b_1 s_1)x + \cdots + b_l s_{k-1} x^{k+l-1}
\end{align*}
\]

so that we are looking to solve

\[
\begin{align*}
a_0 r_0 + b_0 s_0 &= 1, \\
a_0 r_1 + a_1 r_0 + b_0 s_1 + b_1 s_0 &= 0, \\
&\vdots \\
a_k r_{l-1} + b_l s_{k-1} &= 0.
\end{align*}
\]

This system can be expressed by a matrix called the Sylvester matrix

\[
S(f, g) = \begin{pmatrix}
a_0 & 0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\
a_1 & a_0 & 0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\
\vdots & a_1 & a_0 & \cdots & \cdots & b_1 & \cdots & 0 \\
\vdots & \vdots & a_1 & \cdots & \cdots & \cdots & \cdots & 0 \\
a_k & \cdots & a_0 & \cdots & \cdots & b_0 \\
0 & a_k & \cdots & \cdots & b_1 & \cdots & b_1 \\
0 & 0 & a_k & \cdots & 0 & b_1 & \cdots & \cdot \\
\vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \cdots & \cdots & \cdot \\
0 & 0 & \cdots & a_k & 0 & 0 & \cdots & b_l
\end{pmatrix}
\]

and a matrix equation

\[
S(f, g) \begin{bmatrix}
r_0 \\
r_1 \\
\vdots \\
r_{l-1} \\
s_1 \\
\vdots \\
s_{k-1}
\end{bmatrix} = \begin{bmatrix} 1 \\
0 \\
\vdots \\
0 \end{bmatrix}. \] (2)

Warning: The Sylvester matrix depicted above is an approximation, you should think about what it looks like and get your own mental picture. Note that if \( \gcd(f, g) \neq 1 \) then \( S(f, g) \) is certainly singular since (2) has no solution. On the other hand, by exercise A11.4.5 above if \( f \) and \( g \) are relatively prime then (2) has a unique solution and therefore \( S(f, g) \) is nonsingular.
(If a matrix $M$ is singular then there are solutions to $Mx = 0$ with $x \neq 0$ therefore if $Mv = b$ and $Mx = 0$ then $M(x+y) = b$ as well so no solutions to matrix equations are unique.) The resultant promised above is just $R(f, g) = \det S(f, g)$. In summary, $R(f, g) = 0$ if and only if $f$ and $g$ have a common factor.

**A11.6 Bollobás’s Theorem via resultants**

An application of resultants we can give a second linear algebra proof of Bollobás’s Theorem, due to Aart Blokhuis. Recall the theorem:

**Theorem A11.6.1.** If $A_1, \ldots, A_m$ and $B_1, \ldots, B_m$ are sets with $|A_i| = r$ and $|B_j| = s$ such that

$$A_i \cap B_j = \begin{cases} \emptyset & i = j \\ \neq \emptyset & i \neq j \end{cases}.$$ 

Then $m \leq \binom{r + s}{r}$.

**Blokhuis’s Proof.** Without loss of generality assume that $A_i$ and $B_j$ are sets of real numbers. Let $f_i(x) = \prod_{\alpha \in A_i} (x - \alpha)$ and $g_j(x) = \prod_{\beta \in B_j} (x - \beta)$. Then $f_i(x)$ and $g_j(x)$ have a common factor if and only if $i \neq j$. In the language of resultants $R(f_i, g_j) = 0$ if and only if $i \neq j$.

Consider a generic polynomial $G(x) = b_0 + b_1 x + \cdots + b_s x^s$ and observe that $F_i(b_0, \ldots, b_s) = R(f_i, G)$ is a homogeneous polynomial in the $b_i$ of degree $r$. Let $g_j(x) = g_{j0} + g_{j1} x + \cdots + g_{js} x^s$. Because $F_i(g_{j0}, \ldots, g_{js}) \neq 0$ if and only if $i = j$, we see in the usual manner that the $F_i$ are linearly independent. Therefore $m \leq \dim H_r(s+1) = \binom{r+s}{r}$. 

\[\Box\]