1. Motivation

Commutative algebra is largely motivated by the technical demands of *algebraic geometry* and *algebraic number theory.*

1.1. Algebraic geometry.

Consider the space $\mathbb{C}^n$ and the polynomial ring $A = \mathbb{C}[x_1, \dots x_n]$ in n variables. Let $X \subseteq A$ and define

$$V(X) = \{\vec{a} \in \mathbb{C}^n : \forall f \in X \; f(\vec{a}) = 0\}$$

Sets of this kind are called *varieties.*

A little thought shows that $V(X) = V(I)$ where I is the ideal of A generated by X. So we only need study $V(I)$ when I is an ideal.

1.2. Algebraic number theory.

Let $f \in \mathbb{Q}[x]$ and let $\alpha_1, \dots \alpha_m$ be some roots of f. Let F be the least subfield of $\mathbb{C}$ containing the α_i then $\mathbb{Q} \subseteq \mathbb{F}$ and F is a typical *number field.*

Cultural note: This is a serviceable but ugly definition of "number field".. It is equivalent to looking at subfields F of $\mathbb{C}$ which are finite dimensional as $\mathbb{Q}$-vector spaces.

We say that $\alpha \in \mathbb{C}$ is an *algebraic integer* iff α is a root of some monic $f \in \mathbb{Z}[x]$. The algebraic integers form a subring of $\mathbb{C}$ and the algebraic integers in $\mathbb{Q}$ are precisely the elements of $\mathbb{Z}$. If F is a number field then *the ring of integers of F* consists of those $a \in F$ which are algebraic integers.

1.3. Prime ideals.

We spend a great deal of time in this course on prime ideals. Here is some motivation.

[Geometric] The *irreducible varieties* are those of form $V(P)$ for P prime in $A = \mathbb{C}[x_1, \dots x_n]$. Every variety can be written as a finite union of irreducible varieties in an essentially unique way

[Arithmetic] If R is the ring of integers in a number field F then R need not be a UFD **but** every ideal I with $0 \neq I \neq R$ can be written uniquely as a product of prime ideals of R.

2. A theorem on UFDs

.

Theorem 1. *If R is a UFD then $R[x]$ is a UFD.*

Proof. Let F be the field of fractions of F, then $R \leq R[x] \leq F[x]$ where both R and $F[x]$ are UFDs (R by hypothesis and $F[x]$ because F is a field).

We need to be careful because the meaning of the terms "unit" and "irreducible" varies between R, $R[x]$ and $F[x]$.

Easily

1. The units of $R[x]$ are the units of R (since R is an ID).
2. If $r \in R$ then r is irreducible in R iff r is irreducible in $R[x]$.
3. The units of $F[x]$ are the units of F, that is all nonzero elements of F.
4. If $r \in R$ is irreducible in R then r is irreducible in $R[x]$ but a unit in $F[x]$.

We see soon that irreducibles of $R[x]$ with degree nonzero remain irreducible in $F[x]$ and are (up to associates) the only irreducibles in $F[x]$.

We need a technical idea (primitivity) and an important result by Gauss.

If $f \in R[x]$ we say that f is *primitive* iff $f \neq 0$ and 1 is a gcd for the coefficients of f, or equivalently there is no irreducible p of R which divides f in $R[x]$.

Lemma 1. *(Gauss' lemma) The product of two primitive polynomials is primitive.*

$\square$