250B: Commutative Algebra

Nir Elber

Spring 2022

Contents

Theme 1: Introduction

Hold tight to your geometric motivation as you learn the formal structures which have proved to be so effective in studying fundamental questions.

—Ravi Vakil

1.1 January 18

So it begins.

1.1.1 Logistics

Here are some logistic things.

- We are using Eisenbud's *Commutative Algebra: With a View Toward Algebraic Geometry*. We will follow it pretty closely.
- All exams will be open-book and at-home. The only restrictions are time constrains (1.5 hours, 1.5 hours, and 3 hours).
- The first homework will be posted on Monday, and it will be uploaded to bCourses.
- Supposedly there will be a reader for the course, but nothing is known about the reader.

1.1.2 Rings

Commutative algebra is about commutative rings.

Convention 1.1. All of our rings will have a 1_R element and be commutative, as God intended. We do permit the zero ring.

We are interested in particular kinds of rings. Here are some nice rings.

Integral domain

Definition 1.2 (Integral domain)**.** An *integral domain* is a (nonzero) ring R such that, for $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

Units

Definition 1.3 (Units)**.** Given a ring R, we define the group of *units* $R^\times$ to be the set of elements of R which have multiplicative inverses.

Field

Definition 1.4 (Field)**.** A *field* is a nonzero ring R for which $R = \{0\} \cup R^\times$.

Reduced

Definition 1.5 (Reduced)**.** A ring R is *reduced* if and only if it has no nonzero nilpotent elements.

Local

Definition 1.6 (Local)**.** A ring R is *local* if and only if it has a unique (proper) maximal ideal.

It might seem strange to have lots a unique maximal ideal; here are some examples.

Example 1.7. Any field is a local ring with maximal ideal $\{0\}$.

Example 1.8. The ring of p-adic integers $\mathbb{Z}_p$ is a maximal ring with maximal ideal (p).

Example 1.9. The ring $\mathbb{Z}/p^2\mathbb{Z}$ is a local ring with maximal ideal $p\mathbb{Z}/p^2\mathbb{Z}$.

1.1.3 Ideals

The following is our definition.

Ideal

Definition 1.10 (Ideal)**.** Given a ring R, a subset $I \subseteq R$ is an *ideal* if it contains 0 and is closed under R-linear combination.

Given a ring R, we will write

$$(S) \subseteq R$$

to be the ideal generated by the set $S \subseteq R$.

Finitely generated

Definition 1.11 (Finitely generated)**.** An ideal $I \subseteq R$ is said to be *finitely generated* if and only if there are finitely many elements $r_1, \dots, r_n \in R$ such that $I = (r_1, \dots, r_n)$.

Principal

Definition 1.12 (Principal)**.** An ideal $I \subseteq R$ is *principal* if and only if there exists $r \in R$ such that $I = (r)$.

We mentioned maximal ideals above; here is that definition.

Maximal

Definition 1.13 (Maximal)**.** An ideal $I \subseteq R$ is *maximal* if and only if $I \neq R$ and, for any ideal $J \subseteq R$, $I \subseteq J$ implies $I = J$ or $I = R$.

Alternatively, an ideal $I \subseteq R$ is maximal if and only if the quotient ring R/I is a field. We will not show this here.

Prime

Definition 1.14 (Prime)**.** An ideal $I \subseteq R$ is *prime* if and only if $I \neq R$ and, for $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

Again, we can view prime ideals by quotient: I is prime if and only if R/I is a (nonzero) integral domain.

With the above definitions in mind, we can define the following very nice class of rings.

Principal ideal

Definition 1.15 (Principal ideal)**.** An integral domain R is a *principal ideal domain* if and only if all ideals of R are principal.

Example 1.16. The ring $\mathbb{Z}$ is a principal ideal domain. The way this is showed is by showing $\mathbb{Z}$ is Euclidean. Explicitly, fix $I \subseteq \mathbb{Z}$ an ideal. Then if $I \neq (0)$, find an element of $m \in I$ of smallest absolute value and use the division algorithm to write, for any $a \in I$,

$$a = mq + r$$

for $0 \leq r < m$. But then $r \in I$, so minimality of m forces $r = 0$, so $a \in (m)$, finishing.

Example 1.17. For a field k, the ring $k[x]$ is a principal ideal domain. Again, this is because $k[x]$ is a Euclidean domain, where we measure size by degree.

1.1.4 Unique Factorization

We have the following definition.

Irreducible, prime

Definition 1.18 (Irreducible, prime)**.** Fix R a ring and $r \in R$ an element.

- We say that $r \in R$ is *irreducible* if and only if r is not a unit, not zero, and $r = ab$ for $a, b \in R$ implies that one of a or b is a unit.
- We say that $r \in R$ is *prime* if and only if r is not a unit, not zero, and (r) is a prie ideal: $ab \in (r)$ implies $a \in (r)$ or $b \in (r)$.

This gives rise to the following important definition.

Unique factorization domain

Definition 1.19 (Unique factorization domain)**.** Fix R an integral domain. Then R is a *unique factorization domain* if and only if all nonzero elements of R have a factorization into irreducible elements, unique up to permutation and multiplication by units.

Remark 1.20. Units have the "empty" factorization, consisting of no irreducibles.

Example 1.21. The ring $\mathbb{Z}$ is a unique factorization domain. We will prove this later.

Note there are two things to check: that the factorization exists and that it is unique. Importantly, existence does not imply uniqueness.

Exercise 1.22. There exists an integral domain R such that every element has a factorization into irreducibles but that this factorization is unique.

Proof. Consider the subring $R := k\left[x^2, xy, y^2\right] \subseteq k[x, y]$. Here x^2, xy, y^2 are all irreducibles because the only way to factor a quadratic nontrivially would be into linear polynomials, but R has no linear polynomials.

However, these elements are not prime:

$$x^2 \mid xy \cdot xy$$

while x^2 does not divide xy. More concretely, $(xy)(xy) = x^2 \cdot y^2$ provides non-unique factorization into irreducibles. ■

The following condition will provide an easier check for the existence of factorizations.

Ascending chain condition

Definition 1.23 (Ascending chain condition)**.** Given a collection of sets $\mathcal{S}$, we say that $\mathcal{S}$ *has the ascendinc chain condition* (ACC) if and only every chain of sets in $\mathcal{S}$ must eventually stablize.

Example 1.24 (ACC for principal ideals)**.** A ring R has the ascending chain condition for principal ideals if and only if every ascending chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

has some N such that $(a_N) = (a_n)$ for $n \geq N$.

Now, the fact that $\mathbb{Z}$ is a unique factorization domain roughly comes from the fact that $\mathbb{Z}$ is a principal ideal domain.

Theorem 1.25. Fix R a ring. Then R is a principal ideal domain implies that R is a unique factorization domain.

Proof. We start by showing that R has the ascending chain for principal ideals. Indeed, suppose that we have some ascending chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots.$$

Then the key idea is to look at the union of all these ideals, which will be an ideal by following the chain condition. However, R is a principal ideal domain, so there exists $b \in R$ such that

$$\bigcup_{k=1}^{\infty} (a_k) = (b).$$

However, it follows $b \in (a_N)$ for some N, in which case $(a_n) = (a_N)$ for each $n \geq N$.

We can now show that every nonzero element in R has a factorization into irreducibles.

Lemma 1.26. Suppose that a ring R has the ascending chain condition for principal ideals. Then every nonzero element of R has a factorization into irreducibles.

Proof. Fix some $r \in R$. If $(r) = R$, then r is a unit and hence has the empty factorization.

Otherwise, note that every ideal can be placed inside of a maximal and hence prime ideal, so say that $(r) \subseteq \mathfrak{m}$ where $\mathfrak{m}_1$ is prime; because R is a principal ring, we can say that $\mathfrak{m} = (\pi_1)$ for some $\pi_1 \in R$, so $\pi_1 \mid r$. This π_1 should go into our factorization, and we have left to factor r/π_1.

The above argument can then be repeated for r/π_1, and if r/π_1 is not a unit, then we get an irreducible π_2 and consider $r/(\pi_1\pi_2)$. This process must terminate because it is giving us an ascending chain of principal ideals

$$(r) \subseteq \left(\frac{r}{\pi_1}\right) \subseteq \left(\frac{r}{\pi_1\pi_2}\right) \subseteq \cdots,$$

which must stabilize eventually and hence must be finite. Thus, there exists N so that

$$\left(\frac{r}{\pi_1\pi_2\cdots\pi_N}\right) = R,$$

so $r = u\pi_1\pi_2\cdots\pi_N$ for some unit $u \in R^\times$. ∎

It remains to show uniqueness of the factorizations. The main idea is to show that all prime elements of R are the same as irreducible ones. One direction of the implication does not need the fact that R is a principal ring.

Lemma 1.27. Fix R an integral domain. Then any prime $r \in R$ is also irreducible.

Proof. Note that r is not a unit because it is prime. Now, suppose that $r = ab$ for $a, b \in R$; this implies that $r \mid ab$, so because r is prime, without loss of generality we force $r \mid a$. Then, dividing by r (which is legal because R is an integral domain), we see that

$$1 = (a/r)b,$$

so b is a unit. This finishes showing that r is irreducible. ∎

Warning 1.28. The reverse implication of the above lemma is not true for arbitrary integral domains: in the ring $\mathbb{Z}[\sqrt{-5}]$, there is the factorization

$$\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) = 2 \cdot 3.$$

One can show that all elements above are irreducible, but none of them are prime.

The other side of this is harder. Pick up some $\pi \in R$ which is irreducible, and we show that π is prime. In fact, we will show stronger: we will show that (π) is a maximal ideal. Note $(\pi) \neq R$ because π is not a unit.

Indeed, suppose that $(\pi) \subseteq (r)$ for some ideal $(r) \subseteq R$. Then

$$\pi = rs$$

for some $s \in R$. Now, one of r or s must be a unit (π is irreducible). If s is a unit, then $(\pi) = (r)$; if r is a unit then $(r) = R$. This finishes showing that (π) is maximal.

From here we show the uniqueness of our factorizations. We proceed inductively, noting that two empty factorizations are of course the same up to permutation and units. Now suppose we have two factorizations of irreducibles

$$\prod_{k=1}^{m} p_k = \prod_{\ell=1}^{n} q_\ell,$$

where $k + \ell \geq 1$. Note that we cannot have exactly one side with no primes because this would make a product of irreducibles into 1, and irreducibles are not units.

Now, consider p_m. It is irreducible and hence prime and hence divides one of the right-hand factors; without loss of generality $p_m \mid q_n$. But (p_m) and (q_n) are both maximal ideals, so $(p_m) \subseteq (q_n)$ forces equality, so p_m/q_n is a unit. So we may cross off p_m and q_n and continue downwards by induction. ∎

1.1.5 Digression on Gaussian Integers

As an aside, the study of unique factorization came from Gauss's study of the Gaussian integers.

Gaussian integers

Definition 1.29 (Gaussian integers)**.** The *Gaussian integers* are the ring

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

One can in fact check that $\mathbb{Z}[i]$ is a principal ideal domain, which implies that $\mathbb{Z}[i]$ is a unique factorization domain. The correct way to check that $\mathbb{Z}[i]$ is a principal ideal domain is to show that it is Euclidean.

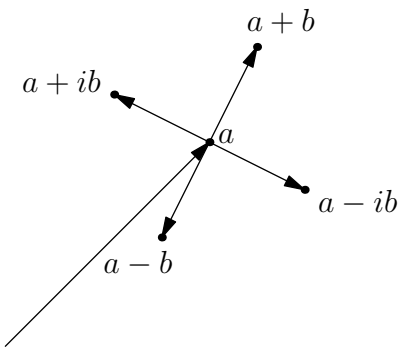
Lemma 1.30. The ring $\mathbb{Z}[i]$ is Euclidean, where our norm is $\mathrm{N}(a+bi) := a^2 + b^2$. In other words, given $\alpha, \beta \in \mathbb{Z}[i]$, we need to show that there exists $q \in \mathbb{Z}[i]$ such that

$$a = bq + r$$

where $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(\beta)$.

Proof. The main idea is to view $\mathbb{Z}[i] \subseteq \mathbb{C}$ geometrically as in $\mathbb{R}^2$. We may assume that $|\beta| \leq |\alpha|$, and then it suffices to show that in this case we may find q so that $a - bq$ has smaller norm than a and induct.

Well, for this it suffices to look at $a + b, a - b, a + ib, a - ib$; the proof that one of these works essentially boils down to the following image.



Note that at least one of the endpoints here has norm smaller than a. ■

What about the primes? Well, there is the following theorem which will classify.

Theorem 1.31 (Primes in $\mathbb{Z}[i]$)**.** An element $\pi := a+bi \in \mathbb{Z}[i]$ is *prime* if and only if $\mathrm{N}(\pi)$ is a $1 \pmod 4$ prime, $(pi) = (1+i)$, or $(\pi) = (p)$ for some prime $p \in \mathbb{Z}$ such that $p \equiv 3 \pmod 4$.

We will not fully prove this; it turns out to be quite hard, but we can say small things: for example, $3 \pmod 4$ primes p remain prime in $\mathbb{Z}[i]$ because it is then impossible to solve

$$p = a^2 + b^2$$

by checking $\pmod 4$.

Remark 1.32. This sort of analysis of "sums of squares" can be related to the much harder analysis of Fermat's last theorem, which asserts that the Diophantine equation

$$x^n + y^n = z^n$$

for $xyz \neq 0$ integers such that $n > 2$.

1.1.6 Noetherian Rings

We have the following definition.

Noetherian ring

Definition 1.33 (Noetherian ring)**.** A ring R is said to be *Noetherian* if its ideals have the ascending chain condition.

There are some equivalent conditions to this.

Proposition 1.34. Fix R a ring. The following conditions are equivalent.

- R is Noetherian.
- Every ideal of R is finitely generated.

Proof. We show the directions one at a time.

- Suppos that R has an ideal which is not finitely generated, say $J \subseteq R$. Then we may pick up any $a_1 \in J$ and observe that $J \neq (a_1)$.

  Then we can pick up $a_2 \in J \setminus (a_1)$ and observe that $J \neq (a_1, a_2)$. So then we pick up $a_3 \in J \setminus (a_1, a_2)$ and continue. This gives us a strictly ascending chain

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots,$$

contadicting the ascending chain condition.

- Suppose that every ideal is finitely generated. Then, given any ascending chain of ideals

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

we need this chain to stabilize. Well, the union

$$I := \bigcup_{k=1}^{\infty} I_k$$

is also an ideal, and it must be finitely generated, so suppose $I = (a_1, a_2, \ldots, a_m)$. However, each a_k must appear in some $I_\bullet$ (and then each $I_\bullet$ after that one as well); choose N large enough to that $a_k \in I_N$ for each k. This implies that, for any $n \geq N$,

$$I_n \subseteq I = (a_1, a_2, \ldots, a_m) \subseteq I_N \subseteq I_n$$

verifying that the chain has stabilized. ■

A large class of rings turn out to be Noetherian, and in fact oftentimes Noetherian rings can build more Noetherian rings.

Proposition 1.35. Fix R a Noetherian ring and $I \subseteq R$ an ideal. Then R/I is also Noetherian.

Proof. Any chain of ideals in R/I can be lifted to a chain in R by taking pre-images along $\varphi : R \twoheadrightarrow R/I$. Then the chain must stabilize in R, so they will stabilize back down in R/I as well. ■

The above works because quotienting is an algeebraic operation. In contrast, merely being a subring is less algebraic, so it is not so surpsising that $R_1 \subseteq R_2$ with R_2 Noetherian does not imply that R_1 is Noetherian.

Example 1.36. The ring $k[x_1, x_2, \ldots]$ is not Noetherian because we have th infinite ascending chain

$$(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots.$$

Howver, $k[x_1, x_2, \ldots] \subseteq k(x_1, x_2, \ldots)$, and the latter ring is Noetherian because it is a field. (Fields are Noetherian because they have finitely many ideals and therefore satisfy the ascending chain condition automatically.)

Here is another way to generate Noetherian rings.

Theorem 1.37 (Hilbert basis)**.** If R is a Noetherian ring, then $R[x]$ is also a Noetherian ring.

Corollary 1.38. By induction, if R is Noetherian, then $R[x_1, x_2, \ldots, x_n]$ is Notherian for any finite n.

Warning 1.39. Again, it is not true that $R[x_1, x_2, \ldots]$ is Noetherian, even though "inducting" with the Hilbert basis theorem might suggest that it is.

Proof of Theorem 1.37. The idea is to use the degree of polynomials to measure size. Fix $I \subseteq R[x]$ an ideal, and we apply the following inductive process.

- Pick up $f_1 \in I$ of minimal degree in I.
- If $I = (f_1)$ then stop. Otherwise find $f_2 \in I \setminus (f_1)$ of minimal degree.

- In general, if $I \neq (f_1, \ldots, f_n)$, then pick up $f_{n+1} \in I \setminus (f_1, \ldots, f_n)$ of minimal degree.

Importantly, we do not know that there are only finitely many $f_\bullet$ yet.

Now, look at the leading coefficients of the $f_\bullet$, which we name $a_\bullet$. However, the ideal

$$(a_1, a_2, \ldots) \subseteq R$$

must be finitely generated, so there is some finite N such that

$$(a_1, a_2, \ldots) = (a_1, a_2, \ldots, a_N).$$

To finish, we claim that

$$I \stackrel{?}{=} (f_1, f_2, \ldots, f_N).$$

Well, suppose for the sake of contradiction that we had some $f_{N+1} \in I \setminus (f_1, f_2, \ldots, f_N)$ of least degree. We must have $\deg f_{N+1} \geq \deg f_\bullet$ for each $f_\bullet$, or else we contradict the construction of $f_\bullet$ as being least degree.

To finish, we note $a_{N+1} \in (a_1, a_2, \ldots, a_N)$, so we are promised constants $c_1, c_2, \ldots, c_N$ such that

$$a_{N+1} = \sum_{k=1}^{N} c_k a_k.$$

In particular, the polynomial

$$g(x) := f_{N+1}(x) - \sum_{k=1}^{N} c_k a_k x^{(\deg g) - (\deg f_k)} f_k(x),$$

will be gauarnteed to kill the leading term of $f_{N+1}(x)$. But $g \equiv f_{N+1} \pmod{I}$, so g is suddenly a polynomial also not in I while of smaller degree than f_{N+1}, which is our needed contradiction. ■

1.1.7 Modules

To review, we pick up the following definition.

Module

Definition 1.40 (Module)**.** Fix R a ring. Then M is an abelian group with an R-action. Explicitly, we have the following properties; fix any $a, b \in R$ and $m, n \in M$.

- $1_R m = m$.
- $a(bm) = (ab)m$.
- $(a + b)m = am + bm$.
- $a(m + n) = am + an$.

Example 1.41. Any ideal $I \subseteq R$ is an R-module. In fact, ideals exactly correspond to the R-submodules of R.

Example 1.42. Given any two R-module M with a submodule $N \subseteq M$, we can form the quotient M/N.

Modules also have a notion of being Noetherian.

Noetherian module

Definition 1.43 (Noetherian module)**.** We say that an R-module M is *Noetherian* if and only if all R-submodules of M are finitely generated.

Remark 1.44. Equivalently, M is Noetherian if and only if the submodules of M have the ascending chain condition. The proof of the equivalence is essentially the same as Proposition 1.34.

Because modules are slightly better algebraic objects than rings, we have more ways to stitch modules together and hence more ways to make Noetherian modules. Here is one important way.

Proposition 1.45. Fix a short exact sequence

$$0 \to A \to B \to C \to 0$$

of R-modules. Then B is Noetherian if and only if A and C are both Noetherian.

Proof. We will not show this here; it is on the homework. Nevertheless, let's sketch the forwards direction, which is easier. Take B Noetherian.

- To show that A is Noetherian, it suffices to note that any submodules $M \subseteq A$ will also be a submodule of B and hence be finitely generated because B is Noetherian.
- To show that C is Noetherian, we note that C is essentially a quotient of B, so we can proceed as we did in Proposition 1.35.[1] ■

Because we like Noetherian rings, the following will be a useful way to make Noetherian modules from them.

Proposition 1.46. Every finitely generated R-module over a Noetherian ring R is Noetherian.

Proof. If M is finitely generated, then there exists some $n \in \mathbb{N}$ and surjective morphism

$$\varphi : R^n \twoheadrightarrow M.$$

Now, because R is Noetherian, R^n will be Noetherian by an induction: there is nothing to say when $n = 1$. Then the inductive step looks at the short exact sequence

$$0 \to R \to R^n \to R^{n-1} \to 0.$$

Here, the fact that R and R^{n-1} are Noetherian implies that R^n is Noetherian by Proposition 1.45. Anyways, the point is that M is the quotient of a Noetherian ring and hence Noetherian by Proposition 1.45 (again). ■

Here is the analogous result for algebras.

Algebra

Definition 1.47 (Algebra)**.** An *R-algebra* S is a ring equipped with a homomorphism $\iota : R \to S$. Equivalently, we may think of an R-algebra as a ring with an R action.

Proposition 1.48. Fix R a Noetherian ring. Then any finitely generated R-algebra is Noetherian.

Proof. Saying that S is a finitely generated R-algebra (with associated map $\iota : R \to S$) is the same as saying that there is a surjective morphism

$$\varphi : R[x_1, \dots, x_n] \twoheadrightarrow S$$

for some $n \in \mathbb{N}$. (Explicitly, $\varphi|_R = \iota$, and each x_k maps to one of the finitely many generating elements of S.) But then S is the quotient of a $R[x_1, \dots, x_n]$, which is Noetherian by Corollary 1.38, so S is Noetherian as well. ■

[1] In fact, Proposition 1.35 is exactly this in the case where $B = R$.

1.1.8 Invariant Theory

In our discussion, fix k a field of characteristic 0, and let G be a finite group or $\mathrm{GL}_n(\mathbb{C})$ (say). Now, suppose that we have a map

$$G \to \mathrm{GL}_n(k).$$

Then this gives $k[x_1, \dots, x_n]$ a G-action by writing $gf(\vec{x}) := f(g^{-1}\vec{x})$. The central question of invariant theory is then as follows.

Question 1.49 (Invariant theory)**.** Fix everything as above. Then can we describe $k[x_1, \dots, x_n]^G$?

By checking the group action, it is not difficult to verify that $k[x_1, \dots, x_n]^G$ is a subring of $k[x_1, \dots, x_n]$. For brevity, we will write $R := k[x_1, \dots, x_n]$.

Here is a result of Hilbert which sheds some light on our question.

Theorem 1.50 (Hilbert's finiteness)**.** Fix everything as above with G finite. Then $R^G = k[x_1, \dots, x_n]^G$ is a finitely generated k-algebra and hence Noetherian.

Proof. We follow Eisenbud's proof of this result. We pick up the following quick aside.

Lemma 1.51. Fix everything as above. If we write some $f \in R^G$ as

$$f = \sum_{d=0}^{\deg f} f_d$$

where f_d is homogeneous of degree d (i.e., f_d contains all terms of f of degree d), then $f_d \in R^G$ as well.

Proof. Indeed, multiplication by $\sigma \in G$ will not change the degree of any monomial (note G is acting as $\mathrm{GL}_n(k)$ on the variables themselves), so when we write

$$\sum_{d=0}^{\deg f} \sigma f_d = \sigma f = f = \sum_{d=0}^{\deg f} f_d,$$

we are forced to have $\sigma f_d = f_d$ by degree comparison arguments. ∎

Remark 1.52. In other words, the above lemma asserts that R^G may be graded by degree.

The point of the above lemma is that decomposition of an element $f \in R^G$ into its homogeneous components still keeps the homogeneous components in R^G, which is a fact we will use repeatedly.

We now proceed with the proof. The main ingredients are the Hilbert basis theorem and the Reynolds operator. Here is the Reynolds operator.

Reynolds operator

Definition 1.53 (Reynolds operator)**.** Fix everything as above. Then, given $f \in R$, we define the *Reynolds operator* $\varphi : R \to R$ as

$$\varphi(f) := \frac{1}{\#G} \sum_{\sigma \in G} \sigma f.$$

Note that division by $\#G$ is legal because k has characteristic zero.

It is not too hard to check that $\varphi : R \to R^G$ and $\varphi|_{R^G} = \mathrm{id}_{R^G}$. Additionally, we see $\deg \varphi(f) \leq \deg f$.

Let $\mathfrak{m} \subseteq R^G$ be generated by the homogeneous elements of R^G of positive degree. The input by the Hilbert basis theorem is to say that $\mathfrak{m}R \subseteq R$ is an R-ideal, and R is Noetherian (by the Hilbert basis theorem!), so $\mathfrak{m}R$ is finitely generated. So set

$$\mathfrak{m}R = (f_1, \dots, f_n) = f_1 R + \cdots + f_n R.$$

By decomposing the $f_\bullet$ into their (finitely many) homogeneous components, we may assume that the $f_\bullet$ are homogeneous.

Now we claim that the $f_\bullet$ generate R^G (as a k-algebra). Note that there is actually nontrivial difficulty turning the above finite generation of $\mathfrak{m}R$ as an R-module into finite of R^G as a k-algebra and that these notions are nontrivially different. I.e., we are claiming

$$R^G \stackrel{?}{=} k[f_1, \dots, f_n].$$

Certainly we have $\supseteq$ here. For $\subseteq$, we show that any $f \in R^G$ lives in $k[f_1, \dots, f_n]$ by induction. By decomposing f into homogeneous parts, we may assume that f is homogeneous.

We now induct on $\deg f$. If $\deg f = 0$, then $f \in k \subseteq k[f_1, \dots, f_n]$. Otherwise, f is homogeneous of positive degree and hence lives in $\mathfrak{m}$. In fact, $f \in \mathfrak{m}R$, so we may write

$$f = \sum_{i=1}^{n} g_i f_i.$$

Note that, because f and f_i are all homogeneous, we may assume that the g_i is also homogeneous because all terms in g_i of degree not equal to

$$\deg f - \deg f_i$$

will have to cancel out in the summation and hence may as well be removed entirely. In particular, each g_i has $g_i = 0$ or is homogeneous of degree $\deg f - \deg f_i$, so $\deg g_i < \deg f$ always.

We would like to finish the proof by induction, noting that $g_i \in R^G$ and $\deg g_i < \deg f$ forces $g_i \in k[f_1, \dots, f_n]$, and hence $f \in k[f_1, \dots, f_n]$ by summation. However, we cannot do that because we don't actually know if $g_i \in R^G$! To fix this problem, we apply the Reynolds operator, noting

$$f = \varphi(f) = \sum_{i=1}^{n} \varphi(g_i) f_i.$$

So now we may say that $\varphi(g_i) \in R^G$ and $\deg \varphi(g_i) < \deg f$, so $\varphi(g_i) \in k[f_1, \dots, f_n]$, and hence $f \in k[f_1, \dots, f_n]$ by summation. This finishes. ∎

The main example here is as follows.

> **Exercise 1.54.** Let S_n act on $R := k[x_1, \dots, x_n]$ as follows: $\sigma \in S_n$ acts by $\sigma x_m := x_{\sigma m}$. Then we want to describe R^G, the *homogeneous polynonmials in n letters*.

Proof. We won't work this out in detail here, but the main point is that the fundamental theorem of symmetric polynomials tells us that

$$R^G = k[e_1, e_2, \dots, e_n],$$

where the $e_\bullet$ are *elementary symmetric functions*. Namely,

$$e_m := \sum_{\substack{S \subseteq \{1,\dots,n\} \\ \#S = m}} \prod_{s \in S} x_s.$$

It is quite remarkable that R^G turned out to be a freely generated k-algebra, just like R. ∎

Here is more esoteric example.

Exercise 1.55. Let $G =: \{1, g\} \cong \mathbb{Z}/2\mathbb{Z}$ act on $R := k[x, y]$ by $g \cdot x = -x$ and $g \cdot y = -y$. Then we want to describe R^G.

Proof. Here, R^G consists of all polynomials $f(x, y)$ such that $f(x, y) = f(-x, -y)$. By checking coefficients of the various $x^m y^n$ terms, we see that $f(x, y) = f(-x, -y)$ is equivalent to forcing all terms of odd degree to have coefficient zero.

In other words, the terms of even degree are the only ones which can have nonzero coefficient. Each such term $x^a y^b$ (taking $a \geq b$ without loss of generality) can be written as

$$x^a y^b = x^{a-b}(xy)^b = \left(x^2\right)^{(a-b)/2} (xy)^b,$$

where $a - b \equiv a + b \equiv 0 \pmod 2$ justifies the last equality. so in fact we can realize R^G as

$$R^G = k\left[x^2, xy, y^2\right].$$

To see that this ring is Noetherian, we note that there is a surjection

$$\varphi : k[u, v, w] \to k\left[x^2, xy, y^2\right]$$

taking $u \mapsto x^2$ and $v \mapsto xy$ and $w \mapsto y^2$. Thus, R is the quotient of a Noetherian ring and hence Noetherian itself. In fact, we can check that[2] $\ker \varphi = \left(uw - v^2\right)$ so that

$$R^G \cong \frac{k[u, v, w]}{(uw - v^2)}.$$

Even though R^G is Noetherian, it is not a freely generated k-algebra (i.e., a polynomial ring over k) because it is not a unique factorization domain! ■

Next class we will start talking about the Nullstellensatz, which has connections to algebraic geometry.

[2] Certainly $uw - v^2 \in \ker \varphi$. In the other direction, any term $u^a v^b w^c$ can be written $\pmod{uw - v^2}$ as a term not having both u and w. However, each $x^d y^e$ has a unique representation in exactly one of the ways $u^a v^b \mapsto x^{2a+b} y^b$ ($a > 0$) or $v^b w^c \mapsto x^b y^{b+2c}$ ($c > 0$) or $v^b \mapsto x^b y^b$, so after applying the $\pmod{uw - v^w}$ movement, we see that the kernel is trivial.