# A Harvard Sampler

Evan Chen

February 23, 2014

I crashed a few math classes at Harvard on February 21, 2014. Here are notes from the classes.

# 1 MATH 123: Algebra II

In this lecture we will make two assumptions.

$$\begin{aligned} \operatorname{char}(F) &= 0 \\ [K : F] &< \infty \end{aligned}$$

Recall that $\operatorname{char}(F) = 0$ means that the sum of $n$ 1's is always nonzero. Also, we deal with finite extensions. We will be using the primitive element theorem a lot. There is a Galois theory of infinite extensions, but not covered here.

Some notes about the notation $F(\cdot)$. If $\alpha \in K$ algebraic over $F$, $K$ is an extension of $F$, then $F(\alpha)$ is the subfield of $K$ generated by $F$. On the other hand, $F(x)$ is the field of rational functions (ratios of polynomials) of $x$ if $x$ is not *a priori* something in a large field $F$.

## 1.1 Review

**Definition 1.1.** A splitting field of a polynomial $p(X)$ over a field $F$ is a field extension K of F over which $p$ factors into linear factors

$$p(X) = \prod_{i=1}^{\deg(p)} (X - a_i) \in K[X]$$

and such that the roots $a_i$ generate $K$ over $F$.

From last lecture we had the following.

**Theorem 1.2** (Splitting Theorem)**.** *Let $F \hookrightarrow K$ and suppose $\exists f \in F[x]$ splitting completely over $K$ as*

$$f(x) = \prod (x - \alpha_i).$$

*If $K = F(\alpha_1, \dots, \alpha_n)$, then $K$ splits over many polynomials: if $g \in F[x]$ is any irreducible polynomial with a root in $K$, then $g$ splits completely in $K$.*

Here the roots of $g$ may not necessarily generate $K$.
Here are some basic facts.

- Given $F$, $f \in F[x]$, there exists a splitting field (should be called a splitting extension) $F \hookrightarrow K$. That is, splitting fields exist for any polynomial. You just repeatedly adjoin.

- Take $F \hookrightarrow L \hookrightarrow K$. If $K$ is a splitting field over $F$, then it is a splitting field $F$. This is obvious.
- Any finite $F \hookrightarrow K$ is contained in a splitting field. Indeed, we may put $K = F(\alpha_1, \dots, \alpha_k)$, and take consider
$$g = \prod g_i$$
where $g_i$ is the minimal polynomial of the $\alpha_i$ over $F$. Then $K \hookrightarrow L$ is a splitting field for $g$ in $F$.

At this point the professor makes a remark about "clearly". He mentions that he had a sobering experience in one of his manuscripts where he noticed a false statement; it was preceded by the word "clearly". He then proceeded to search for all other instances of the word "clearly" and found a half-dozen other errors.

## 1.2 Galois Theory

The basic idea of Galois theory: algebraically, it's impossible to distinguish between the different roots of a polynomial in a splitting field.

Explicitly, let $\alpha_1, \dots, \alpha_n$ be the roots of an irreducible polynomial. Consider $K = F(\alpha_1, \dots, \alpha_n)$, and look at its subfields $F(\alpha_1), F(\alpha_2), \dots, F(\alpha_n)$ each themselves an extensions of $F$. The point is that each of these subfields are isomorphic. Now we want to use automorphisms using the irreducibility.

**Definition 1.3.** The *Galois group* $G(K/F)$ is precisely the group of automorphisms of $(K/F)$; that is, it is the set of maps
$$\{\varphi : K \to K \text{ such that } \varphi\,|_F \text{ is the identity}\}$$

## 1.3 Main Theorem

**Theorem 1.4.** *For any finite extension $F \hookrightarrow K$, then*
$$\#G(K/F) \le [K : F].$$
*In fact, the order of the Galois group $G(K/F)$ will divide the degree of the extension $[K : F]$.*

*Moreover, equality holds if and only if $K$ is a splitting field over $F$.*

Henceforth, "splitting fields" will also be known as "Galois extensions". The above theorem is used to characterize Galois extensions! Note that we are being careful to take $\operatorname{char} F = 0$! These two notions become different if $F$ has characteristic $p$.

*Proof.* Say $F \hookrightarrow K$ is a splitting field (hence finite); the other case is pretty similar.

Let $\alpha$ be a generator (primitive element) of $K$ that is, $K = F(\alpha)$. Let $f$ be the minimal polynomial (hence irreducible); the splitting theorem then implies
$$f(x) = \prod_{i=1}^{n} (x - \alpha_i) \in K[x].$$
where of course $\alpha \in \{\alpha_i\}$.

Of course each of the $\alpha_i$ is degree $n$. That means $F(\alpha_i)$ is a degree $n$ extension of $K$ contained in $K$; hence equal to $K$. The whole point is that

$$K = F(\alpha_1, \dots, \alpha_n) \cong F(\alpha_1) \cong \dots \cong F(\alpha_n).$$

Of course these are also isomorphic to $F[x]/(f)$ by $\alpha_i \mapsto x$. The proof is simply that

$$K = F(\alpha_i) \cong F[x]/(f) \cong F(\alpha_j) = K$$

for all $i$, $j$. (The isomorphisms are $x \mapsto \alpha_i$ and $x \mapsto \alpha_j$).

Note that since $K = F(\alpha_i)$, any automorphism of $K/F$ is determined by where it sends any one of the $\alpha_i$.[1] It has no stabilizers – if an automorphism fixes any $\alpha_i$, then it is the identity.[2] Hence $G(K/F) \hookrightarrow S_n$ has an image which is a simply transitive subgroup. Hence $\#G = n = [K : F]$.

What happens if we don't assume $F \hookrightarrow K$ is a splitting extension? (Reversing the assumption at the beginning of the proof.) Let $F \hookrightarrow K$ be any finite extension and put $n = [K : F]$. Let $\alpha \in K$ be a primitive element and set $K = F(\alpha)$, and let $f(x) \in F[x]$ be the irreducible polynomial of $\alpha$ over $F$. We are no longer sure that $f$ splits completely over $F$. But if we let $\alpha_1, \dots, \alpha_k$ be the roots that do live in $K$, then once again we see that $K = F(\alpha_1) = \dots = F(\alpha_k)$. Once again we find that $G(K/F) \hookrightarrow S_k$ and is simply transitive, so $\#G(K, F) = k$. Now just observe $k \le n$. □

Again note that we've been using the primitive element theorem; that is, there exists a primitive element. That's why we need $\text{char}(F) = 0$.

### 1.4 Fixed points of Galois groups

Given a Galois extension $K$ over $F$, let $G = G(K/F)$. By definition, all automorphisms in $G$ fix $F$.

**Proposition 1.5.** *Any element of $\alpha \in K$ fixed by all automorphisms in $G$ is in $F$. In other words, $F$ is the set of fixed points of $K$ under $G$.*

We write this as $F = K^G$. This means we can recover $F$ from $K$ and $G$!

Let's try doing this the other way around!

**Theorem 1.6.** *Let $H$ be any finite group, and $K$ is any field. Suppose $H$ acts on $K$, with $H \hookrightarrow \text{Aut}(K)$. Set $F = K^H$. Then $K/F$ is Galois, with splitting field $G(K/F) = H$.*

This lets us find any intermediate extensions! The end.

## 2 MATH 137: Algebraic Geometry

**Definition 2.1.** The radical $\sqrt{I}$ of an ideal is defined by

$$\left\{x : \exists n : x^n \in I\right\}.$$

In what follows we will assume $S$ is a polynomial ring. We will be interested in varieties $V(I)$, where $I$ is an ideal in $S$. This can be interpreted as the set of points in space which vanish on all the polynomials in the ideal.

[1] It fixes all the things in $F$ by definition. Because it carries $f$ to $f$, it carries a root of $f$ to a root of $f$.

[2] If $\alpha_3$ is fixed by the automorphism, then it fixes everything in $K$, since $K = F(\alpha_3)$.

## 2.1 Primary Ideal

**Definition 2.2.** Recall that $I$ an ideal of any ring $S$ is *primary* if $fg \in I$ implies either $f \in I$ or $g^m \in I$ for some $m$. Equivalently, if $xy \in I$, then $x \in I$, $y \in I$, or $x, y \in \sqrt{I}$.

This is a refinement of *prime* ideal. It's slightly weaker.

Roughly, an ideal is primary if it specifies some higher order vanishing conditions "uniformly" on $V(I)$.

Throughout this lecture $S = k[x_1, \dots, x_n]$ is a polynomial ring we care about.

**Example 2.3.** Let $f(x, y)$ be a nonzero irreducible polynomial and define

$$I = \left\langle f(x,y), z^2 \right\rangle.$$

This ideal is primary (homework), but we claim that $I \cap \langle z \rangle$ is not primary.

**Proposition 2.4.** *Every ideal has a* primary decomposition *– it is an intersection of of primary ideals.*

Say $I$ is *irreducible* if $I = I_1 \cap I_2$ implies that either $I_1 = I$ or $I_2 = I$.

**Claim 2.5.** Let $I$ be irreducible. Then it's primary.

*Proof.* Consider the quotient (colon ideal) chain

$$I : g \subseteq I : g^2 \subseteq \dots.$$

This is an ascending chain contained within $I$, so it eventually stabilizes. That means $I : g^N = I : g^{N+1}$ for some $N$.

Now we claim that

$$(I + \left\langle g^N \right\rangle) \cap (I + \langle f \rangle) = I.$$

If so, then irreducibility will force $I + \left\langle g^N \right\rangle = I$, and hence $g^N \in I$.

Take $h = a + bg^N = c + df$, where $a, c \in I$ and $b, d \in S$. Once we show $h \in I$ we're done. Product by $g$ gives

$$hg = ag + bg^{N+1} = cg + dfg.$$

Since $fg \in I \Rightarrow dfg \in I$. Now $ag, cg \in I$ gives $bg^{N+1} \in I$. Now use the ascending chain condition to get $b \in I : g^{N+1} = I : g^N$. □

*Proof.* By standard argument, we can write $I = \bigcap Q_i$ for $Q_i$ irreducible, since otherwise we can just get an infinite chain. Now this gives the proposition. □

## 2.2 Minimal decompositions

**Definition 2.6.** A primary decomposition $I = \bigcap Q_i$ is minimal/irredundant if

(a) One cannot delete any of the $Q_i$'s and get the same result

(b) All the radicals $\sqrt{Q_i}$ are distinct.

Recall that $\sqrt{Q_i}$ is prime, and $Q_i$ is "$\sqrt{Q_i}$-primary" (whatever that means).

**Lemma 2.7.** *If $I$, $J$ are $P$-primary, then $I \cap J$ is $P$-primary.*

**Example 2.8.** Let $I = (x, y^2)$, $J = (x^2, y)$, and $P = (x, y)$. Then $I \cap J = (x^2, xy, y^2)$.

*Proof.* Exercise. □

**Theorem 2.9** (LN)**.** *Every proper ideal has a minimal primary decomposition.*

The idea is that given a primary decomposition, we use the lemma to intersect anything appearing more than once. Then throw out redundant terms.

### 2.3 Associated Primes

Recall our example $I = \langle f(x,y), z^2 \rangle$. We can decompose it as the intersection of the plane and the $f(x,y)$ zero locus from whatever.

**Theorem 2.10.** *If $I = \cap Q_i$ If $I = \cap Q_i$ is a minimal primary decomposition, then the prime ideals $\sqrt{Q_i}$ are precisely the primes in the set*

$$\left\{ \sqrt{I : f} \mid f \in S \right\}.$$

Apparently things that are defined by $\sqrt{Q}$ are "flat" in some sense.

The point is that even though primary decompositions need not be unique, the associated primes are unique and hence depend only on $I$. Here is an example.

$$I = (xy, y^2) = (y) \cap (x, y^2) = (y) \cap (x^2, xy, y^2).$$

This means something geometrically, but I can't tell what it is. The associated primes are $(y)$ and $(x,y)$ in both cases (line and point).

We have uniqueness in some cases though.

**Definition 2.11.** The minimal element of a set of associated primes $\mathcal{P}$ are called *isolated*/minimal primes/components. The others are called *embedded*.

**Example 2.12.** In our example, $(xy, y^2)$ breaks into two things. Here the guy with $(x,y)$ prime can vary, since it depends only on what it induces in $(y)$. ON the other hand $(y)$ can't change.

**Fact 2.13.** If $\sqrt{Q_i}$ is minimal in a primary decomposition $\bigcap Q_i$, then this $Q_i$ is uniquely determined.

This lecture was the last in which we describe the objects we study in algebraic geometry (varieties). In future lectures we discuss regular mappings between varieties.

## 3 Math 129: Algebraic Number Theory

Warning: the other two lectures before this sort of made sense to me. This one was all symbols.

### 3.1 Review

Last time we stated the following theorem.

**Theorem 3.1.** *Let $A$ be a Dedekind domain, and $K$ a fraction field.*

*(a) The set of fractional ideals of $A$ is a group under multiplication.*

*(b) For any fractional ideal $b$ there is a unique factorization*

**Proposition 3.2.** *If $m \subset A$ is a maximal ideal and $m' = \{x \in K : xm \subset A\}$ then $m'$ is a fractional ideal and $mm' = A$.*

There are two lemmas involved.

**Lemma 3.3.** *If a prime $p \subset A$ contains a product of ideals $Q_1 \dots Q_n$, then it contains $Q_i$ for some $i$.*

**Lemma 3.4.** *Any nonzero ideal in $A$ contains a nonzero product of primes.*

## 3.2 Some proofs

Now we prove the proposition.

*Proof.* First, we claim that $m' \not\subseteq A$. Pick $0 \neq a \in m$ and observe that by the second lemma,

$$p_1 p_2 \dots p_r \subset (a) \subset m.$$

By Lemma 2, we may assume $p_1 \subset m$ (since some prime does, WLOG it is $p_1$). Hence $p_1 = m$.

Suppose that the collection $\{p_1, \dots, p_r\}$ is minimal with respect to the property $p_1 p_2 \dots p_r \subset (a)$. Then $p_1 p_2 \dots p_m$ is not contained in $A$.

Then $b = p_2 p_3 \dots p_m$ is not contained in $(a)$, so $\exists t \in b - (a)$. On the other hand

$$tm \subset bm \subset bp_1 \subset (a)$$

hence $a^{-1}bm \in A$ but $a^{-1}b \not\in A$; hence $a^{-1}b \in m - A$.

If $mm' = m$, then for every $x \in m'$ we have $xm \subset m \Rightarrow x^n m \subset m$ for all $n \geq 0$. Thus $A[x] \subset K$ is integral over $A$. Hence $x \in A$ because $A$ is an integrable integrably closed; this is a contradiction since $m' \not\subset A$. □

Now we prove the theorem.

*Proof.* We will first show that every ideal $b$ has a product decomposition

$$b = \prod_p p^{n_p(pb)}.$$

We may assume that $b \subset A$; otherwise $\exists d \in A$ such that $b \subseteq d^{-1}A$; hence we may write $b = (db)(dA)^{-1}$. This is the same as saying $db \subseteq A$, then we can express $db$ is a product of primes, and hence $b$. This is the first reduction.

Hence we only need to prove the claim when $b$ is an ideal. The assertion is trivially true for maximal ideals. Hence given $b \subset A$ we can assume that every ideal containing $b$ strictly admits a product decomposition (in the style of induction).

Pick a maximal prime $p \subset A$ containing $b$. Then we have the fractional ideal $p'$ such that $pp' = A$. We know that $p' \not\subset A$. Hence $b \subsetneq p$, so if $x \in p' - A$ then $xb \subseteq A$. Hence $p'b \subseteq A$. Since $1 \; inp'$, so $b \in p'b \subseteq A$.

Now we claim that $b \subsetneq p'b$. This is basically the same argument as before – if not we can find $x \in p' - A$ such that $xb \subset b$ implying $x^n b \subset b$ for all $n$. Hence $A[x] \subseteq K$ is a fractional ideal, meaning $A[x]$ is integral over $A$; thus $x \in A$ by integral closure, contradiction.

Now we're basically done. $b \subsetneq p'b \subset A$ gives $p'b = \prod_q q^{n_q(pb)}$ admits a composition because it strictly contains $b$. Hence $b = Abpp'b = b\prod_q q^{n_q(p'b)}$, showing part (a).

To show uniqueness, we mimic the proof in $\mathbb{Z}$. □

**Corollary 3.5.** *Given two ideals $a, b \subset A$, we have $a \subset b$ for all maximal ideas $p \subset A$ if and only if $n_p(A) \geq n_p(b)$.*

*Proof.* Blah. □

## 3.3 An Example

**Example 3.6.** Let $K = \mathbb{Q}(\zeta_p)$, where $\zeta_p$ is a $p$th root of unity.

Note that $\zeta_p$ is a root of the irreducible polynomial $f(x) = x^{p-1} + \cdots + 1$. One can show that $A$, the ring of the integers in $K$, is precisely equal to

$$A = \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[x]/(f(x)).$$

We want to like find the factorization of the principle ideal $(p)$ generated inside of $A$. It's convenient toput $x = y + 1$, so that

$$\frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = y^p + \sum_{i=1}^{p-1} \binom{p}{i} y^{i-1}.$$

So let's call $g(y) = y^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} y^{i-1}$. Then $A = \mathbb{Z}[y]/g(y)$.

So what is $A/pA$?. It is

$$A/pA = \mathbb{Z}[y]/(g(y), p) = \mathbb{F}_p[y]/(y^{p-1}).$$

Since, after all $g(y)$ disappears modulo $p$.

Now $y = \zeta_p - 1$ and hence

$$A/(\zeta_p - 1)A = \mathbb{Z}[y]/(g(y), y) = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

wat. Okay so $(\zeta_p - 1)A$ is prime.

Apparently this gives $(\zeta_p - 1)^{p-1} \in pA$. Hence

$$(\zeta_p - 1)^{p-1} A \subseteq pA \subseteq (\zeta_p - 1)A.$$

That implies in turn that $pA = (\zeta_p - 1)^e A$ for some $0 \le e \le p - 1$.

On the other hand, $A/(\zeta_p - 1)^p A = \frac{\mathbb{F}_p[y]}{/} y^e$.

This is called a *ramification*. You take $p$, look at how it decomposes in $\mathbb{Z}[\zeta_p]$. They all collapse into one prime. It turns out that essentially $p$ is the only prime with that property. The end.