Galois Theory

Course Notes

22 February 2016 – 24 April 2016

1 About This Course

1.1 Suggested Reading

S. Lang, *Algebra* (3rd ed., 2002) Contains many exercises. Parts V, VI, and VII are especially relevant.

R. Elkik, *Cours d'algebre* (2002) In French. Closest in content to this course.

J. S. Milne, *Fields and Galois Theory* (2015) Course notes. Available for free on the Web at http://www.jmilne.org/math/CourseNotes/ft.html. The last three chapters contain "interesting and important material" not covered in the course.

I. Stewart, *Galois Theory* (2015) Less technically ambitious than this course, but includes history, and other applications such as ruler-and-compass constructions.

2 Week 1 Notes: 22 Feb – 28 Feb

2.1 Field extensions. Examples.

This course assumes a basic knowledge of abstract algebra (groups, rings, fields, modules), and linear algebra. All rings we consider will be associative, commutative, and with unity.

2.1.1 Two definitions of field extension.

Let K and L be fields.

Definition 1. We say that L is an **extension of** K if $K \subset L$. That is, K is a subfield of L. Equivalently, L is an extension of K if L is a K**-algebra**—in other words, if we have $(k_1\mathbf{a_1})(k_2\mathbf{a_2}) = k_1k_2\mathbf{a_1}\mathbf{a_2}$ for $k_i \in K$ and $\mathbf{a_i} \in A$.

Why are these definitions equivalent? In fact, given a K-algebra structure on a ring A, this is the same as having a homomorphism of rings $f : K \to A$. So if we have a K-algebra, define a homomorphism f by setting $f(k) = k\mathbf{1}$ for $k \in K$. Conversely, given an arbitrary homomorphism $f : K \to A$, set $k\mathbf{a} = f(k)\mathbf{a}$ for $\mathbf{a} \in A$.

Suppose now that $A = L$ a field. Then any homomorphism $f : K \to L$ is injective. There are several ways to see this; for example, we can show that $f(k)$ is always invertible. Indeed, $\mathbf{1} = f(1) = f(kk^{-1}) = f(k)f(k^{-1})$ for any $k \neq 0$, so $f(k) \neq \mathbf{0}$ whenever k is nonzero. Alternatively, we know that the kernel of f is always an ideal. But L is a field, so the only ideals of L are (0) and $(1) = K$.

2.1.2 Three examples.

Example 1. $\mathbb{C}$ is an extension of $\mathbb{R}$, and $\mathbb{R}$ is an extension of $\mathbb{Q}$.

Example 2. If L is a field, then either (a) $1 + 1 + \ldots + 1 \neq 0$ for any sum of 1's. Then L has characteristic 0 and so we have $\mathbb{Z} \subset L$, which means $\mathbb{Q} \subset L$. Then L is an extension of $\mathbb{Q}$. Alternatively, suppose (b) $1 + 1 + \cdots + 1 = 0$ for some finite m number of terms. The minimal such number for which this is true turns out to necessarily be a prime, p. We then say that L has characteristic p, and so we have $\mathbb{Z}/p\mathbb{Z} \subset L$; $\mathbb{Z}/p\mathbb{Z}$ is a field, and we denote it (with field structure) by $\mathbb{F}_p$. In this case L is an extension of $\mathbb{F}_p$. We call $\mathbb{Q}$ and $\mathbb{F}_p$ the **prime fields**: any field is an extension of a prime field, and prime fields don't contain any proper subfields.

Example 3. Take $K[x]/(P)$, the ring of polynomials in one variable over K, modded out by the ideal of an irreducible polynomial P. This is a field. Suppose $Q \notin (P)$, then $\gcd(Q, P) = 1$, so for some polynomials A, B we have $AP + BQ = 1$ by Bézout's identity. Hence $BQ \equiv 1 \pmod{P}$, that is, B is an inverse of Q in $K[x]/(P)$.

2.2 Algebraic elements. Minimal polynomial.

We continue with the previous example: the quotient $K[x]/(P)$ is a field. Rather than Bézout's identity, we can say that (P) is a **maximal ideal** of $K[x]$, and the quotient of a ring by a maximal ideal is always a field. The proof of this fact uses the same identity.

This field is an extension of K in the obvious way: it is a K-algebra!

2.2.1 A concrete example.

Let $K = \mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$, and $P = x^2 + x + 1$. Then $K[x]/(P)$ contains four elements: 0, 1, the class containing x (denoted by $\bar{x}$, and the class containing $x + 1$ (denoted by $\overline{x+1}$). We have that $\bar{x}^2 = -\bar{x} - 1 = \overline{x+1}$ since K has characteristic 2. Similarly $(\overline{x+1})^2 = \bar{x}$. Moreover, these elements are inverses of each other: $\bar{x}(\overline{x+1}) = \bar{x}^2 + \bar{x} = -1 = 1$. Since $|K[x]/(P)| = 4$, we write $K[x]/(P) = \mathbb{F}_4$. This notation seems presumptuous, implying that there is "only" one field with four elements: in fact every field with a given finite number of elements is isomorphic, so this is true. A proof will come later.

2.2.2 Algebraic elements of a field extension.

Example 4. Given a field extension $K \subset L$ and an element $\alpha \in L$, we say that α is **algebraic** if there exists some polynomial $P \in K[x]$ such that $P(\alpha) = 0$; if no such polynomial exists, we say that α is **transcendental**.

Lemma 1. *If α is algebraic, then there exists a* unique *unitary polynomial P of minimal degree with $P(\alpha) = 0$. P is irreducible, and for any Q such that $Q(\alpha) = 0$, then Q is divisible by P.*

Definition 2. We call such a polynomial P the **minimal polynomial of α over K**, denoted $P_{\min}(\alpha, K)$.

Proof of lemma. We know that $K[x]$ is a **principal ideal domain**, and the polynomials $I = \{Q \in K[x] : Q(\alpha) = 0$ forms an ideal. Thus I has a generator, so $I = (P)$ for some P. This generator is a unique (up to a constant) element of minimal degree in I. Furthermore, if P was *not* irreducible—if $P = QR$—then $P(\alpha) = Q(\alpha)R(\alpha)$ and so at least one of $Q(\alpha) = 0$ or $R(\alpha) = 0$. This would contradict the minimal-degree condition on P. ■

2.3 Algebraic elements. Algebraic extensions.

2.3.1 An important bit of notation.

Definition 3. We denote by $K(\alpha)$ the smallest subfield of L containing α. We say that $K[\alpha]$ (note the square braces) is the smallest subring (or K-algebra) containing K and α.

$K[\alpha]$ is generated, as a vector space over K, by $1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots$.

Example 5. $\mathbb{C} = \mathbb{R}(\imath)$ as a field, but also $\mathbb{C} = \mathbb{R}[\imath]$ as a ring. Every $z \in \mathbb{C}$ can be written $z = x + \imath y$; this is a vector subspace generated by $1, \imath$.

Proposition 1. *The following are equivalent: (1) α is algebraic over K; (2) $K[\alpha]$ is a finite dimensional vector space over K; (3) $K[\alpha] = K(\alpha)$.*

Proof. (1) $\Rightarrow$ (2): We have that $\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + \alpha_1\alpha + a_0 = 0$ for $a_i \in K$ (this is just the minimal polynomial). Then $\alpha^d = -\left(\sum_{k=0}^{d-1} a_k\alpha^k\right)$, a linear combination of the lower powers of α. Therefore $K[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{d-1}$ over K: it is finite-dimensional.

(2) $\Rightarrow$ (3): It is enough to prove that $K[\alpha]$ is a field, since $K[\alpha] \subset K(\alpha)$. Let $x \in K[\alpha]$ nonzero. We want to show that x is invertible. Consider the operation of multiplication by x, that is, $y \mapsto xy$ for $y \in K[\alpha]$: this is an injective homomorphism of vector spaces over K. But as $K[\alpha]$ is finite-dimensional, this is also a surjection, so there exists $z \in K[\alpha]$ such that $xz = 1$. Hence x is invertible, and so $K[\alpha]$ is a field.

(3) $\Rightarrow$ (1): If α is not algebraic, then there exists no polynomial P such that $P(\alpha) = 0$. This means that the natural homomorphism $i : K[x] \to L$ defined by $P \mapsto P(\alpha)$ is injective, but $K[\alpha]$ is *not* a field, and the image of i is a field. Contradiction! ■

2.3.2 Definition and properties of algebraic extensions.

Definition 4. L is called **algebraic** over K if every element of L is algebraic over K.

Proposition 2. *If L is algebraic over K, then any K-subalgebra of L is a field.*

Proof. Let $L' \subset L$ be a subalgebra. We know that $\alpha \in L'$ algebraic. Then $K[\alpha] \subset L$ is a field, so α is invertible (when nonzero). This holds for any such (nonzero) α, so L' is a field. ■

Proposition 3. *If $K \subset L \subset M$, and $\alpha \in M$ is algebraic over K, then α is algebraic over L and its minimal polynomial $P_{\min}(\alpha, L)$ divides $P_{\min}(\alpha, K)$.*

Proof. Consider $P_{\min}(\alpha, K)$ as an element of $L[x]$. ■

2.4 Finite extensions. Algebraicity and finiteness.

2.5 Algebraicity in towers. An example.

2.6 A digression: Gauss lemma, Eisenstein criterion.