Galois Theory

Course Notes

22 February 2016 – 24 April 2016

Contents

Part I

Notes

1 Lecture Notes: 22 Feb – 28 Feb

1.1 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.

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 $(1) = K$.

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 $K[x]/(P)$.

1.2 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!

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.

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. ■

1.3 Algebraic elements. Algebraic extensions.

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! ■

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 $L[x]$. ■

1.4 Finite extensions. Algebraicity and finiteness.

Definition 5 (Finite extension)**.** L is said to be a **finite extension** of K if it is a finite-dimensional K-vector space. The dimension of L over K is called the **degree** of L over K, and is denoted by $[L : K]$.

Theorem 1. *Suppose $K \subset L \subset M$. Then M is finite over K if and only if M is finite over L and L is finite over K. Moreover, in this case, the degrees multiply: $[M : K] = [M : L][L : K]$.*

Proof of Thm. 1. First, suppose M is finite over K. Then any linearly independent family $\{m_i\}$ over L are also linearly independent over K, so $\dim_L M$ is finite. Now L is a K-vector subspace of M, so $\dim_K M$ is finite and thus $\dim_K L$ is finite.

Second, let $\{e_i\}_{i=1}^n$ be an L-basis of M, and $\{\varepsilon_j\}_{j=1}^d$ a K-basis of L. We want to show that $e_i\varepsilon_j$ form a K-basis of M. Indeed, for any $x \in M$, we have that $x = \sum_i a_i e_i$ with $a_i \in L$. And for each i, $a_i = \sum_j b_{ij}\varepsilon_j$ with $\sum_{i,j} b_{ij}\varepsilon_j \in K$. So we can write $x = \sum_{i,j} b_{ij}\varepsilon_j e_i$, showing that $e_i\varepsilon_j$ generate M over K. We now need to verify that these elements are linearly independent over K.

If we have $\sum_{i,j} c_{ij} e_i \varepsilon_j = 0$ then $\sum_i \left(\sum_j c_{ij}\varepsilon_j\right) e_i = 0$, and $\sum_j c_{ij}\varepsilon_j \in L$. But $\{e_i\}$ is a basis, so for all i, we have $\sum_j c_{ij}\varepsilon_j = 0$. And since $\{\varepsilon_j\}$ is a basis, necessarily $c_{ij} = 0$ for all i, j. This proves the theorem. ■

Definition 6. We say that $K(\alpha_1, \ldots, \alpha_n) \subset L$, the smallest subfield of L containing $K, \alpha_1, \ldots, \alpha_n$, is **generated** by $\alpha_1, \ldots, \alpha_n$ over K.

Theorem 2. *L is finite over K if and only if L is generated by a finite number of algebraic elements over K.*

Proof. First, suppose that $\{\alpha_i\}_{i=1}^d$ is a K-basis of L. Then $L = K[\alpha_1, \ldots, \alpha_d] = K(\alpha_1, \ldots, \alpha_d)$. Moreover, each $K[\alpha_i]$ is a finite-dimensional K-algebra since it is a subring of (already finite-dimensional) L. Then by Proposition 1, α_i is algebraic.

Second, suppose $K[\alpha_1]$ is finite dimensional over K; $K[\alpha_1, \alpha_2]$ is finite dimensional over $K[\alpha_1]$; ...; $K[\alpha_1, \ldots, \alpha_{d-1}, \alpha_d]$ finite dimensional over $K[\alpha_1, \ldots, \alpha_{d-1}]$. Each α_i is algebraic, so for $1 \leq i \leq d$ we have $K[\alpha_1, \ldots, \alpha_i] = K(\alpha_1, \ldots, \alpha_i)$. Now we use Theorem 1 to conclude that $L = K(\alpha_1, \ldots, \alpha_d)$ is finite over K. ■

1.5 Algebraicity in towers. An example.

Algebraic extensions have a similar property to finite extensions: a tower of extensions is algebraic only if the floor of the tower is algebraic.

Theorem 3. *Let $K \subset L \subset M$. Then M is algebraic over K if and only if M is algebraic over L and L is algebraic over K.*

Proof. First, let $\alpha \in M$. If $P(\alpha) = 0$ for some $P \in K[x]$, then also $P \in L[x]$, so α is algebraic over L. Now if $\alpha \in L$ then also $\alpha \in M$ and so α is algebraic over K. Thus L is algebraic over K.

Second, suppose L is algebraic over K and M is algebraic over L; we need to show that M is algebraic over K. Take $\alpha \in M$ and consider $P_{\min}(\alpha, L)$. Its coefficients are elements of L, so they are algebraic over K. By the previous theorem, they generate an extension, E, which is *finite* over K. Now $E(\alpha)$ is also finite over K. Since $E(\alpha)$ is finite over E, then α is algebraic over K: there exists a linear dependence relation between powers of α. ■

We now consider an example.

Example 6. Consider $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. This is clearly algebraic and finite over $\mathbb{Q}$. The degree of this extension is 6: we have $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. The minimal polynomial $P_{\min}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$; $\mathbb{Q}(\sqrt[3]{2})$ is generated over $\mathbb{Q}$ by 1, $\sqrt[3]{2}$, $(\sqrt[3]{2})^2$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Now $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2})$, because otherwise we would have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt[3]{2})$. Then $2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ would divide $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, which is impossible. Therefore, $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$, and so is in fact the minimal polynomial for $\sqrt{3}$ over this extension.

The degree of the big extension, $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$, and therefore $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = (2)(3) = 6$.

In fact, this reflects a more general property:

Proposition 4. *If α is algebraic over K, then the degree of $K(\alpha)$ over K is equal to the degree of the minimal polynomial of α over K.*

Proof. The proof is obvious: $K(\alpha)$ is generated by the powers of α up to some α^{d-1} (if $\deg P_{\min}(\alpha, K) = d$), and these are linearly independent. ■

This gives us a nice tool to compute the degree of algebraic extensions.

Proposition 5. *Let $K \subset L$ be a field extension and let $L' = \{\alpha \in L : \alpha$ is algebraic over $K\}$. Then L' is a subfield of L; we call this the* ***algebraic closure*** *of K in L.*

Proof. Let α, β be algebraic over K. We want to show that $\alpha + \beta$ and $\alpha\beta$ are algebraic; these facts follow immediately from Theorem 2, since $\alpha + \beta$ and $\alpha\beta$ belong to $K[\alpha, \beta]$, which is a finite (by Theorem 2) extension of K. ■

1.6 A digression: Gauss lemma, Eisenstein criterion.

A brief review.

We said that for a field K, an element α is algebraic over K if α is a root of some polynomial $P \in K[x]$.

We said that an extension L is algebraic over K if every element $\alpha \in L$ is algebraic over K.

We said that L is finite over K if the dimension of L over K is finite.

We saw that finite implies algebraic, and that we have finiteness if and only if the field is algebraic *and* finitely generated.

Finally, we deduced that $[K(\alpha) : K] = \deg P_{\min}(\alpha, K)$.

Therefore, it's important to be able to know whether a given polynomial is in fact irreducible over K.

How to decide that a polynomial is irreducible over K.

In our example we had $x^3 - 2$ is irreducible $\mathbb{Q}$. Since the degree of this polynomial is equal to 3 and there is no root in $\mathbb{Q}$.

But if we ask whether $x^{100} - 2$ is irreducible over $\mathbb{Q}$, this is not so trivial. In fact it is irreducible, based on a few facts.

Lemma 2 (Gauss)**.** *Let $P \in \mathbb{Z}[x]$. If P decomposes nontrivially (that is, $P = QR$, where $\deg Q, \deg R < \deg P$) over $\mathbb{Q}$, then it also decomposes over $\mathbb{Z}$.*

Proof. Let $P = QR$. Set $mQ = Q_1 \in \mathbb{Z}[x]$ and $nR = R_1 \in \mathbb{Z}[x]$. Then $mnP = Q_1R_1 \in \mathbb{Z}[x]$. For $p|mn$, then modulo p we have $0 = \bar{Q}_1\bar{R}_1$. Since we're working over $\mathbb{F}_p$ a field, we have that $\bar{Q}_1 = 0 \pmod p$ or $\bar{R}_1 = 0 \pmod p$: that is, p divides all of the coefficients of either Q_1 or R_1. WLOG say this is Q_1. Then $\frac{mn}{p}P = Q_2R_1 \in \mathbb{Z}[x]$ where $Q_2 = \frac{Q_1}{p}$. Continuing in this way, we arrive at $P = Q_lR_s \in \mathbb{Z}[x]$. ■

Example 7 (Eisenstein criterion example)**.** To show that $x^{100} - 2$ is irreducible over $\mathbb{Z}$? We reduce modulo 2: if $x^{100} - 2 = QR$ then $x^{100} = \bar{Q}\bar{R}$ in $\mathbb{F}_2[x]$, so $\bar{Q}$ and $\bar{R}$ are of the form x^k respectively x^l. The constant coefficients of both $\bar{Q}$ and $\bar{R}$ must be divisible by 2; hence the constant coefficient of $x^{100} - 2$ must be divisible by 4, except this is not the case. Therefore

Proposition 6 (Eistenstein criterion)**.** *Let $P \in \mathbb{Z}[x]$ with $P = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$. If there exists a prime p such that (1) p divides a_n; (2) p divides a_i for $i = 0, \ldots, n-1$; and (3) p^2 does not divide a_0; then $P \in \mathbb{Z}[x]$ is irreducible.*

Proof. The proof is the same as in the example. ■

Both facts are valid in more generality, by replacing $\mathbb{Z}$ with any unique factorization domain R, and replacing $\mathbb{Q}$ by the fraction field of R.

1.7 Week 1 Quiz

1. Which of the following are true?

A finite extension of fields is algebraic. This is *true*.

An algebraic extension of fields is finite. T his is *false*; for example, the field of all algebraic numbers is an infinite extension of $\mathbb{Q}$.

A finitely generated and algebraic extension of fields is finite. This is *true*.

2. Which of the following pairs is an extension of fields?

$\mathbb{Z}, \mathbb{Q}$ is *not* a field extension because $\mathbb{Z}$ is not a field.

$\mathbb{Q}, \mathbb{R}$ is a field extension because $\mathbb{R}$ is a field and $\mathbb{Q} \subset \mathbb{R}$.

$\mathbb{Q}(\imath), \mathbb{R}$ is *not* a field extension because, e.g., $\imath \in \mathbb{Q}(\imath)$ but $\imath \notin \mathbb{R}$, and so $\mathbb{Q}(\imath)$ is not a subfield of $\mathbb{R}$.

$\mathbb{Q}(\imath), \mathbb{C}$ is a field extension because $\mathbb{C}$ is a field and $\mathbb{Q}(\imath) \subset \mathbb{C}$.

3. What is the minimal polynomial of $e^{2\pi\imath/3}$ over $\mathbb{Q}$?

Let $\zeta = e^{2\pi\imath/3}$, and note that $\zeta^3 = e^{2\pi\imath} = 1$. Therefore ζ is a root of the polynomial $Q(x) = x^3 - 1$. Now Q is not irreducible: $Q = PR$, where $P(x) = x^2 + x + 1$ and $R(x) = x - 1$. $R(\zeta) \neq 0$ but $P(\zeta) = 0$, and P is irreducible over Q (by, e.g., the quadratic formula). Therefore $P(x) = x^2 + x + 1$ is the minimal polynomial for ζ over $\mathbb{Q}$.

4. Which of the following polynomials f is irreducible over the specified field K?

$f_1 = x^2 + x + 1$ is irreducible over $K_1 = \mathbb{Q}$; see previous question.

$f_2 = x^2 - 2$ is irreducible over $K_2 = \mathbb{Q}$, since its roots are $\pm\sqrt{2} \notin \mathbb{Q}$.

$f_3 = x^2 - 2$ is *not* irreducible over $K_3 = \mathbb{R}$, since its roots are $\pm\sqrt{2} \in \mathbb{R}$.

$f_4 = x^2 + x + 1$ is *not* irreducible over $K_4 = \mathbb{F}_3$: we have $f_4(1) = 1 + 1 + 1 = 0$ since the field has characteristic 3, and $1 \in \mathbb{F}_3$.

$f_5 = x^4 + 6x^2 + 2$ is irreducible over $K_5 = \mathbb{Q}$. Setting $y = x^2$ and $\hat{f}_5 = y^2 + 6y + 2$, we obtain by the quadratic formula

$$y = \frac{-6 \pm \sqrt{36 - 4}}{2} = \frac{-6 \pm \sqrt{32}}{2} = \frac{-6 \pm 4\sqrt{2}}{2} = -3 \pm 2\sqrt{2},$$

and hence $x = \pm\sqrt{-3 \pm 2\sqrt{2}} \notin \mathbb{Q}$.

$f_6 = x^3 - 1$ is *not* irreducible over $K_6 = \mathbb{Q}$; see previous question.

5. Which of the following quotient rings is a field?

Note that this is equivalent to asking if the polynomial we're modding out by is irreducible over the base field.

$\mathbb{R}[x]/(x^2 - 2)$ is *not* a field, since $x^2 - 2$ is not irreducible over $\mathbb{R}$.

$\mathbb{Q}[x]/(x^2 - 2)$ is a field, since $x^2 - 2$ is irreducible over $\mathbb{Q}$.

$\mathbb{F}_3[x]/(x^2 + x + 1)$ is *not* a field, since $x^2 + x + 1$ is not irreducible over F_3.

$\mathbb{R}[x]/(x^2 - 1)$ is *not* a field, since $x^2 - 1$ is not irreducible over $\mathbb{R}$.

$\mathbb{R}[x]/(x^2 + 1)$ is a field, since $x^2 + 1$ is irreducible over $\mathbb{R}$.

6. What is the degree of the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$?

We know that the extension is generated by products of $1, \sqrt{2}, \sqrt{3}$. Now $1^2 = 1$, $(\sqrt{3})^2 = 3$, $(\sqrt{2})^2 = 2$, and $\sqrt{2}\sqrt{3} = \sqrt{6}$; therefore any element $q \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written $q = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ with $a, b, c, d \in \mathbb{Q}$. Therefore $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

2 Lecture Notes: 29 Feb – 06 Mar

2.1 Stem field. Some irreducibility criteria.

2.1.1 Definition, existence, and uniqueness of stem fields.

Definition 7. Let $P \in K[x]$ be irreducible and monic. A **stem field** for P is an extension $E \supset K$ such that E contains a root α of P and $E = k[\alpha]$.

We know that such a thing exists; take, for example $K[x]/(P)$. This is a field, since P is irreducible. On the other hand, *any* stem field E is isomorphic to $K[x]/(P)$. It's easier to define this isomorphism the other way: $K[x]/(P) \to E$ where $f \mapsto f(\alpha)$.

To summarize, we have the following proposition.

Proposition 7. *A stem field exists, and if E and E' are two stem fields for $P \in K[x]$ generated by roots α and α' respectively, then there exists a* unique *isomorphism of K-algebras $E \to E'$ taking $\alpha \mapsto \alpha'$.*

Proof. We've already shown existence. Proving the uniqueness of the isomorphism is also easy. We know that any isomorphism of $K[\alpha]$ with E' is defined by the value it takes on α. Now, we have $\varphi : K[x]/(P) \to E$ and $\psi : K[x]/(P) \to E'$, so take $\psi^{-1} \circ \varphi : E \to E'$. This is an isomorphism, and since φ maps $x \mapsto \alpha$ and ψ maps $x \mapsto \alpha'$ we see that $\psi^{-1} \circ \varphi$ maps $\alpha \mapsto \alpha'$. ■

Remark 1. In particular, if a stem field contains two roots of P, there exists a *unique* automorphism taking one root to the other root.

Remark 2. If E is a stem field, then $[E : K] = \deg P$; conversely, if $[E : K] = \deg P$ and E contains a root of P, then E is a stem field. (Otherwise, its degree over K would be strictly greater than the degree of P.)

2.1.2 More criteria for irreducibility.

Corollary 1. A polynomial $P \in K[x]$ is irreducible over K if and only if it does not have roots in extensions $L \supset K$ of degree less than or equal to $n/2$, where $n = \deg P$.

Proof. Suppose P is not irreducible. Then it has a prime factor Q such that $\deg Q \leq n/2$, so we can take L as the stem field of Q.

Conversely, if P has a root $\alpha \in L$, then $P_{\min}(\alpha, K)$ divides P. Then P cannot be irreducible. ■

Corollary 2. Let $P \in K[x]$ be irreducible of degree n, and let L be an extension of degree m. If $\gcd(n, m) = 1$ then P is irreducible over L.

Proof. Suppose Q divides P in $L[x]$. Let M be a stem field of Q over L. We now have $K \subset L \subset M = L[\alpha]$. Then $K(\alpha)$ is a stem field of P over K, so $[K(\alpha) : K] = n$. On the other hand, if $\deg Q = d$, then $[M : L] = d$ since M is a stem field of Q over L. Thus, the total degree $[M : K] = [M : L][L : K] = md$. But $K(\alpha) \subseteq M$, so n must divide md. If $\gcd(n, m) = 1$ then n must divide d, but d doesn't exceed n and so $n = d$. Therefore P is irreducible over L. ■

2.2 Splitting field.

Now let $P \in K[x]$ (not necessarily irreducible).

Definition 8. A field $L \supset K$ is a **splitting field** of P over K if it is an extension where P is **split** (i.e., is a product of linear factors) and if it is generated by the roots of P. (So it is the smallest field in which P splits.)

Theorem 4. *(1) A splitting field exists, and its degree over K is less than or equal to $d!$, where $d = \deg P$; and (2) If L and L' are two splitting fields for P, then there exists an isomorphism of K-algebras $L \to L'$ (but this isomorphism is not necessarily unique).*

Proof. We will proceed by induction on d, the degree of the polynomial $P \in K[x]$.

First, if $d = 1$, then everything is trivial (the splitting field is just K itself).

Now suppose that $d > 1$ and assume the theorem has been proved for all polynomials of degree less than d over any field K. In this case, let Q be an irreducible factor of P and let α be a root of Q. Then $L_1 = K[\alpha]$ is a stem field of Q; over L_1, we have $P = (x - \alpha)R$.

By hypothesis, we know that there exists a splitting field L of R over L_1 and that $[L : L_1] \leq (\deg R)! \leq (d - 1)!$ since $\deg R \leq d - 1$. This will be a splitting field of P over k, and $[L : K] = [L : L_1][L_1 : K] \leq (d - 1)!d = d!$.

It remains to prove uniquness up to isomorphism. Let L and M be two splitting fields. Let β be a root of Q in M, where Q is some irreducible factor of P. Then $K[\alpha]$ and $K[\beta]$ are both stem fields for Q, and we have an isomorphism $\varphi : K[\alpha] \to K[\beta]$ that sends α to β. Now $P = (x - \beta)S$ in $M[x]$, where $S = \varphi(R)$. M is a splitting field of S over $K[\beta]$.

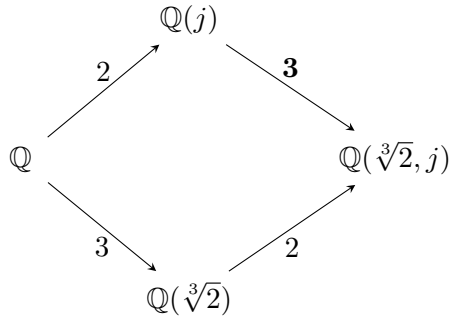
But M is also a $K[\alpha]$-algebra via φ. As such, it is a splitting field of R over $K[\alpha]$. By induction, we have a $K[\alpha]$-isomorphism from L to M, so also we have a K-isomorphism between L and M. ■

Remark 3. This isomorphism is *not unique*! In particular, a splitting field can have many K-automorphisms. This is in fact the subject of Galois theory: the study of the group of automorphisms.

2.3 An example. Algebraic closure.

Consider the polynomial $x^3 - 2$ over $\mathbb{Q}$. Its roots are $\sqrt[3]{2}$, $j\sqrt[3]{2}$, and $j^2\sqrt[3]{2}$, where $j = e^{2\pi\imath/3}$ (i.e. the primitive third root of unity). The splitting field is then $L = \mathbb{Q}(\sqrt[3]{2}, j)$. Let us now find the automorphisms of L.

We have two towers:



The minimum polynomial of j over $\mathbb{Q}$ is $x^2 + x + 1$, and indeed this is also the minimum polynomial over $\mathbb{Q}(\sqrt[3]{2})$ (since, e.g., j is not a real number, so it cannot be in that field). Moreover, we conclude that $[\mathbb{Q}(j, \sqrt[3]{2}) : \mathbb{Q}(j)]$ must be 3, since the total degree is 6, the degree of $\mathbb{Q}(j)$ over $\mathbb{Q}$ is 2, and degrees multiply in towers.

There must exist a $\mathbb{Q}(j)$-automorphism of L, call it σ, taking $\sqrt[3]{2}$ to $j\sqrt[3]{2}$, because L is a stem field of $x^3 - 2$ over $\mathbb{Q}(j)$, so there are automorphisms that interchange roots.

There is also a $\mathbb{Q}(\sqrt[3]{2})$-automorphism of L, call it τ, taking j to j^2, since these are two roots of the same minimal polynomial, and L is a stem field of $x^2 + x + 1$ over $\mathbb{Q}(\sqrt[3]{2})$.

Thus we have a group of automorphisms, $\mathrm{Aut}(L/K)$, embedded in S_3, the group of permutations on 3 elements. In fact, $\mathrm{Aut}(L/K) = S_3$, since σ is a cyclic permutation of roots ($\sqrt[3]{2} \to j^2\sqrt[3]{2} \to \sqrt[3]{2}$) and τ is a transposition that fixes $\sqrt[3]{2}$ and exchanges the other roots ($j\sqrt[3]{2} \leftrightarrow j^2\sqrt[3]{2}$). Together they generate S_3.

2.3.1 Algebraic closure.

Definition 9. A field K is **algebraically closed** if any non-constant polynomial has a root in K. That is, any non-constant polynomial splits in $K[x]$.

Example 8. The field of complex numbers, $\mathbb{C}$, has this property (to be proved later, by "almost" pure algebra).

Definition 10. An **algebraic closure** of K is a field L which is algebraically closed and also algebraic over K.

Theorem 5. *Any field K has an algebraic closure.*

Note that at this point we're saying nothing about *uniqueness*.

Proof. First, we construct K_1 such that for any polynomial $P \in K[x]$ has a root in K_1. This is not yet a victory, because we don't know if any polynomial in $K_1[x]$ has a root in K_1 itself. So we construct K_2 such that any polyomial in $K_1[x]$ has a root in K_2, and so forth. We then have $K \subset K_1 \subset K_2 \cdots \subset K_n \subset \cdots$, and take $\bar{K} = \bigcup K_n$. We now claim that $\bar{K}$ is algebraically closed; indeed, any polynomial $P \in \bar{K}[x]$ really has its coefficients in some "floor" of this tower. So there exists some n such that $P \in K_n[x]$, which implies that P has a root in K_{n+1}, and therefore it has a root in $\bar{K}$. If we learn how to construct these K_1, K_2, and so on, we will have solved the problem.

We proceed with the construction of K_1. Let S be the set of all irreducible elements of $K[x]$, and $A = K[(x_p)_{p \in S}]$, that is, one variable x_p for every $p \in S$. (A is a very big polynomial ring!)

Let $\mathfrak{i} \subset A$ be the ideal generated by all $P(x_p)$, $p \in S$. We claim that $\mathfrak{i}$ is a proper ideal. Indeed, if not, then we can write $1 = \sum_{i=1}^{n} \lambda_i P_i(x_{p_i})$, with the coefficients $\lambda_i \in A$. The main point here is that this sum is *finite*.

Next, take L the splitting field of $\prod_{i=1}^{n} P_i$ over K, and let α_i be a root of P_i in K. Since A is a polynomial ring, it's easy to produce a homomorphism from a polynomial algebra to some other algebra (just note where the mapping sends the variables). Hence there exists a homomorphism $\varphi : A \to L$ sending $x_{p_i} \mapsto \alpha_i$, and all other x_p to 0 (that is, when $p \neq p_i$). Now we have that $\varphi(1) = 0$, since $\varphi(P_i(x_{p_i})) = P_i(\alpha_i) = 0$; this is a contradiction, since we need $\varphi(1) = 1$.

Having shown that $\mathfrak{i}$ is a proper ideal, we use the fact that any such ideal in a commutative associative ring with unity is contained in a maximal ideal $\mathfrak{m}$ and $A/\mathfrak{m}$ is a field. Take $K_1 = A/\mathfrak{m}$, and continue in the same way to construct $K_2, K_3, \ldots, K_n, \ldots$. ∎

Remark 4 (Ideals in a ring). Any proper ideal (in a commutative associative ring with unity) is contained in a maximal ideal. This is a consequence of Zorn's lemma.

Lemma 3 (Zorn)**.** *For $\mathcal{P}$ a partially ordered set, we say that a subset $\mathcal{C} \subset \mathcal{P}$ is a **chain** if, for all $\alpha, \beta \in \mathcal{C}$, we have $\alpha \leq \beta$ or $\beta \leq \alpha$, where $\leq$ is the order relation on $\mathcal{P}$. If any non-empty chain in a non-empty $\mathcal{P}$ has an upper bound, then $\mathcal{P}$ has maximal elements.*

We will not prove Zorn's lemma, since it's equivalent to the Axiom of Choice, or a meta-theorem, etc.: Relevant to set theory and mathematical foundations, but not to Galois theory.

Now, in this case we have $\mathcal{P}$ as the set of all proper ideals in A containing $\mathfrak{i}$. We know $\mathcal{P}$ is non-empty because it contains $\mathfrak{i}$. Any chain $\{\mathfrak{i}_\alpha\}_{\alpha \in J}$ has an upper bound: this is $\bigcup_{\alpha \in J} \mathfrak{i}_\alpha$. (It's easy to check that this is an ideal.) So by Zorn's lemma we know that $\mathcal{P}$ has maximal elements. Then $\mathfrak{i} \subset \mathfrak{m}$ a maximal idea. Then $A/\mathfrak{m}$ is a field. Otherwise, some $a \in A/\mathfrak{m}$ would generate a proper ideal, and its pre-image under $\pi : A \to A/\mathfrak{m}$ would strictly contain $\mathfrak{m}$.

2.4 Extension of homomorphisms. Uniqueness of algebraic closure.

To sum up, we have just proved the existence of an algebraic closure $\bar{K} = \bigcup_{i=1}^{\infty} K_i$ where $K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots$. Each K_i is a field where each $P \in K_{i-1}[x]$ has a root, and was constructed as the quotient of a huge polynomial ring over K_{i-1} by a suitable maximal ideal (first finding a proper ideal, then leveraging Zorn's lemma to find the maximal ideal).

Naturally we might ask if there is a uniqueness result for the algebraic closure. In fact there is, but we need another theorem first.

Theorem 6 (Extension of homomorphisms)**.** *Let $K \subset L \subset M$ be algebraic extensions, and embed $K \hookrightarrow \Omega$ into some algebraic closure (of K). Then any homomorphism $\varphi : L \to \Omega$ extends to a homomorphism $\tilde{\varphi} : M \to \Omega$.*

Proof. We again apply Zorn's lemma, this time to the following set:

$$\mathcal{E} = \{(N, \psi) : L \subset N \subset M, \text{ and } \psi|_L = \varphi\}$$

We know $\mathcal{E}$ is non-empty because it contains (L, φ). We equip $\mathcal{E}$ with a partial order by the following relation: $(N, \psi) \leq (N', \psi')$ if $N \subseteq N'$ and $\psi'|_N = \psi$ (that is, ψ' extends ψ).

Now, any chain (N_α, ψ_α) has an upper bound (N, ψ); we know that the union $N = \bigcup_\alpha N_\alpha$ is a field and a subextension of M. Then ψ is defined in the obvious way (for $x \in N_\alpha$, set $\varphi(x) = \varphi_\alpha(x)$). Hence, by Zorn's lemma we know that $\mathcal{E}$ has maximal elements. Let (N_0, ψ_0) be one such element

and suppose $N_0 \neq M$, that is, the inclusion is strict. To obtain a contradiction, take $x \in M/N_0$ and consider $P_{\min}(x, N_0)$. Let $\alpha \in \Omega$, and define a map $N_0(x) \to \Omega$ by $x \mapsto \alpha$, and equal to ψ_0 on N_0. This contradicts the maximality of the extension ψ_0. Therefore $N_0 = M$, and we take $\tilde{\varphi} = \psi_0$. ■

Corollary 3. If Ω, Ω' are two algebraic closures of K, then the are isomorphic as K-algebras.

Proof (Sketch). Since we have embeddings $i : K \hookrightarrow \Omega$ and $i' : K \hookrightarrow \Omega'$, we can extend i (respectively j) to a map $\varphi : \Omega' \to \Omega$ (respectively, a map $\varphi' : \Omega \to \Omega'$). Combining the two gives an isomorphism between Ω and Ω'. ■

2.5 Week 2 Quiz

⋆1. Which of the following are true?

a. There is a field K and a polynomial $P \in k[x]$ such that P can never be written as a product of linear factors in $F[x]$, no matter how large the extension field F/K. This is *false*; we proved (Thm. 4) that a splitting field for P always exists.

b. If P is an irreducible polynomial of degree d over a field K, then there is a splitting field of P of degree at most d. This is *false*; consider $P = x^3 - 2 \in \mathbb{Q}[x]$, so the splitting field for P is $\mathbb{Q}(\sqrt[3]{2}, j)$ (where j is the primitive third root of unity). Now the splitting field has degree 6, but the polynomial only has degree 3.

c. If P is an irreducible polynomial of degree d over a field K, then there is a splitting field of P of degree at most $d!$ over K. This is *true*; we proved this (Thm. 4).

d. Given an irreducible polynomial P of degree d over a field K, it is possible to have a field extension F/K of degree less than d that contains a root of P. This is *false*: Let α be a root of P. Then the stem field $K(\alpha)$ is generated by $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$, and so has dimension (and degree over K) equal to d; if any of these elements were not in the set, then it wouldn't be a field (e.g., suppose $\alpha^2 \notin K(\alpha)$ with $d = 4$, and therefore $\alpha^3/\alpha = \alpha^2 \notin K(\alpha)$, so the field axioms aren't satisfied).

e. Let P be an irreducible polynomial over a field K, and $K(\alpha)$, $K(\beta)$ be two stem fields for P over K. Then it is possible for there to be two distinct isomorphisms $f, g : K(\alpha) \to K(\beta)$ with $f(\alpha) = g(\alpha) = \beta$. This is *false*; we proved (Prop. 7) that there is a unique such isomorphism.

⋆2. Let F be a splitting field of $x^4 - 2$, constructed as the subfield of $\mathbb{C}$ generated by the roots of $x^4 - 2$. Which of the following are true?

Note that the roots of $x^4 - 2$ are $\sqrt[4]{2}, \imath\sqrt[4]{2}, -\sqrt[4]{2}$, and $-\imath\sqrt[4]{2}$, since $\imath$ and $-\imath$ are the primitive fourth roots of unity. Therefore $F = \mathbb{Q}(\imath, \sqrt[4]{2})$.

a. There is a subfield $E \subset F$ of degree 4 over $\mathbb{Q}$ and containing a root of $x^4 - 2$. This claim is *true*: Since $\sqrt[4]{2}$ is a root of $x^4 - 2$, let $E = \mathbb{Q}(\sqrt[4]{2})$. Then $[E : \mathbb{Q}] = 4$, since E is generated by $\left\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\right\}$ over $\mathbb{Q}$.

b-d. What is the degree of F over $\mathbb{Q}$? The degree of $\mathbb{Q}(\imath, \sqrt[4]{2})$ over $\mathbb{Q}$ is 8, since it's generated by $\left\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3, \imath, \imath\sqrt[4]{2}, \imath\sqrt{2}, \imath(\sqrt[4]{2})^3\right\}$, which is an eight-element basis.

e. F contains the complex number $\imath$. This claim is *true*: $\sqrt[4]{2}, \imath\sqrt[4]{2} \in F$, so $\imath\sqrt[4]{2}/\sqrt[4]{2} = \imath \in F$.

f-g. What is the degree of F over $\mathbb{Q}(\imath)$? We know that $[\mathbb{Q}(\imath) : \mathbb{Q}] = 2$ and $[F : \mathbb{Q}] = 8$, so we must have $[F : \mathbb{Q}(i)] = 4$.

3. Let F be a splitting field of $x^4 - 2$, constructed as the subfield of $\mathbb{C}$ generated by the roots of $x^4 - 2$, and consider the group $G = \mathrm{Aut}(F)$ of automorphisms of the field F. Which of the following are true?

Let $\alpha = \sqrt[4]{2}$. Then the roots of $x^4 - 2$ are $\alpha, \imath\alpha, -\alpha, -\imath\alpha$.

F is generated over $\mathbb{Q}$ by the real root α of $x^4 - 2$ and by the complex number $\imath$: $F = \mathbb{Q}(\alpha, \imath)$. This claim is *true*: see question 2.

There is an automorphism $\varphi \in G$ with $\varphi(\alpha) = \alpha, \varphi(\imath) = -\imath$ and another automorphism ψ with $\psi(\alpha) = \imath\alpha, \psi(\imath) = \imath$. The minimal polynomial for $\imath$ over $\mathbb{Q}$ is $P_{\min}(\imath, \mathbb{Q}) = x^2 + 1$, and in fact this is also the minimal polynomial for $\imath$ over $\mathbb{Q}(\alpha)$ since $\imath$ is imaginary. Therefore, since F is a stem field for $x^2 + 1$ over $\mathbb{Q}(\alpha)$ that contains two roots of $x^2 + 1$ (that is, $\imath$ and $-\imath$, there must exist a $\mathbb{Q}(\alpha)$-automorphism taking $\imath \mapsto -\imath$, by Prop. 7.

Similarly, the minimal polynomial for α over $\mathbb{Q}$ is $P_{\min}(\alpha, \mathbb{Q}) = x^4 - 2$, and this is also the minimal polynomial for α over $\mathbb{Q}(\imath)$ since α is irrational. Therefore, since F is a stem field for $x^4 - 2$ over $\mathbb{Q}(\imath)$ that contains two roots of $x^4 - 2$ (that is, α and $\imath\alpha$, there must exist a $\mathbb{Q}(\imath)$-automorphism taking $\alpha \mapsto \imath\alpha$, by Prop. 7.

This claim is *true*: There must be a $\mathbb{Q}(\alpha)$-automorphism that interchanges roots (i.e. sends $\imath \mapsto -\imath$), and similarly there must be a $\mathbb{Q}(\imath)$-automorphism that interchanges roots (i.e. sends $\alpha \mapsto \imath\alpha$). These automorphisms are precisely φ and ψ.

The subgroup of G generated by φ and ψ is commutative. This claim is *false*. We see that $\varphi(\psi(\alpha)) = \varphi(\imath\alpha) = -\imath\alpha$ whereas $\psi(\varphi(\alpha)) = \psi(\alpha) = \imath\alpha$.

Write $z \in F$ as a linear combination of its generators:

$$z = q_1 + q_2\alpha + q_3\alpha^2 + q_4\alpha^3 + q_5\imath + q_6\imath\alpha + q_7\imath\alpha^2 + q_8\imath\alpha^3$$

Then the automorphisms φ and ψ act on F by:

$$\varphi(z) = q_1 + q_2\alpha + q_3\alpha^2 + q_4\alpha^3 - q_5\imath - q_6\imath\alpha - q_7\imath\alpha^2 - q_8\imath\alpha^3$$

and

$$\begin{aligned}\psi(z) &= q_1 + q_2\imath\alpha + q_3\imath^2\alpha^2 + q_4\imath^3\alpha^3 + q_5\imath + q_6\imath(\imath\alpha) + q_7\imath(\imath^2\alpha^2) + q_8\imath(\imath^3\alpha^3) \\ &= q_1 + q_2\imath\alpha - q_3\alpha^2 - q_4\imath\alpha^3 + q_5\imath - q_6\alpha - q_7\imath\alpha^2 + q_8\alpha^3 \\ &= q_1 - q_6\alpha - q_3\alpha^2 + q_8\alpha^3 + q_5\imath + q_2\imath\alpha - q_7\imath\alpha^2 - q_4\imath\alpha^3\end{aligned}$$

In fact, we can write φ and ψ as matrices under the given basis:

$$M_\varphi = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}, \qquad M_\psi = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Now consider $(\varphi \circ \psi)(\alpha)$ versus $(\psi \circ \varphi)(\alpha)$:

$$(\varphi \circ \psi)(z) = q_1 + q_6\alpha - q_3\alpha^2 - q_8\alpha^3 - q_5\imath + q_2\imath\alpha + q_7\imath\alpha^2 - q_4\imath\alpha^3 \tag{1}$$

$$(\psi \circ \varphi)(z) = q_1 - q_6\alpha - q_3\alpha^2 + q_8\alpha^3 - q_5\imath - q_2\imath\alpha + q_7\imath\alpha^2 + q_4\imath\alpha^3 \tag{2}$$

Since (1) is not equal to (2), we see that this subgroup is not commutative.

The automorphisms of φ and ψ generate a proper subgroup of the group G. This claim is *false*. Let $H = \langle \varphi, \psi \rangle$, the subgroup of G generated by φ and ψ under composition. Let $a = \varphi$ and $b = \varphi \circ \psi$. Then we have that $a^2 = e$ and $b^2 = e$, where e is the identity map; yet $ab \neq ba$. This

describes the dihedral group on 4 elements, D_8: so $H = \langle \varphi, \psi \rangle = \langle a, b | a^2 = e, b^2 = e, ab \neq ba \rangle = D_8$. Now let $\xi \in G$. Then for any $z \in F$ we have:

$$\begin{aligned}
\xi(z) &= \xi(q_1 + q_2\alpha + q_3\alpha^2 + q_4\alpha^3 + q_5\imath + q_6\imath\alpha + q_7\imath\alpha^2 + q_8\imath\alpha^3) \\
&= q_1 + q_2\xi(\alpha) + q_3\xi(\alpha^2) + q_4\xi(\alpha^3) + q_5\xi(\imath) + q_6\xi(\imath\alpha) + q_7\xi(\imath\alpha^2) + q_8\xi(\imath\alpha^3) \\
&= q_1 + q_2\xi(\alpha) + q_3\xi(\alpha)^2 + q_4\xi(\alpha)^3 + q_5\xi(\imath) + q_6\xi(\imath)\xi(\alpha) + q_7\xi(\imath)\xi(\alpha)^2 + q_8\xi(\imath)\xi(\alpha)^3
\end{aligned}$$

So the automorphism is determined by where it sends α and $\imath$. The options are:

$$\begin{aligned}
\alpha \mapsto \alpha, \imath \mapsto \imath &= \xi_0 = e \\
\alpha \mapsto \alpha, \imath \mapsto -\imath &= \xi_1 = a \\
\alpha \mapsto -\alpha, \imath \mapsto \imath &= \xi_2 = abab = baba \\
\alpha \mapsto -\alpha, \imath \mapsto -\imath &= \xi_3 = bab \\
\alpha \mapsto \imath\alpha, \imath \mapsto \imath &= \xi_4 = ba \\
\alpha \mapsto \imath\alpha, \imath \mapsto -\imath &= \xi_5 = b \\
\alpha \mapsto -\imath\alpha, \imath \mapsto \imath &= \xi_6 = ab \\
\alpha \mapsto -\imath\alpha, \imath \mapsto -\imath &= \xi_7 = aba
\end{aligned}$$

Indeed, we cannot send $\imath$ to anything but one of $\pm\imath$ because it has order 2, whereas α has order 4; and we cannot send α to anything but one of $\{\pm\alpha, \pm\imath\alpha\}$ because anything else would either (1) reduce to purely an element of $\mathbb{Q}$; or (2) increase the coefficient, for example $\alpha \mapsto \alpha^3$ results in $q_3\alpha^2 \mapsto q_3\alpha^6 = 2q_3\alpha^2$.

Hence we have enumerated the entire group of automorphisms of F, and this is precisely the group generated by a and b (equivalently, ψ and φ).

There is an injective group homomorphism $G \hookrightarrow S_4$. This claim is *true*. First define a mapping $f : \{1, 2, 3, 4\} \to F$ by $f(1) = \alpha$, $f(2) = \imath\alpha$, $f(3) = -\alpha$, $f(4) = -\imath\alpha$. Then if $* = G \hookrightarrow S_4$, in cycle notation we have $\varphi^* = (2\ 4)$ and $\psi^* = (1\ 2\ 3\ 4)$; since φ and ψ generate G, we have that $G^* \subseteq S_4$. In particular since $G \approx D_8 \subset S_4$ we know we have an injection.

There is a surjective homomorphism $G \hookrightarrow S_4$. This claim is *false*. For example, the permutation (1 2) cannot represent any element of G, as such an element would interchange α and $\imath\alpha$ yet fix $-\alpha$ and $-\imath\alpha$, which is incompatible with their action on the base field F.

⋆4. Which of the following are true?

a. $\mathbb{C}$ is an algebraic closure of $\mathbb{Q}$. This is *false*: $\mathbb{C}$ is bigger than the algebraic closure of $\mathbb{Q}$. Since $\mathbb{Q}$ is countable, we expect $\bar{\mathbb{Q}}$ to also be countable. However, $\mathbb{C}$ is uncountable.

b. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. This is *true*.

c. Given an algebraic extension $F/\mathbb{Q}$, there is a *unique* homomorphism $F \to \mathbb{C}$ of fields. This is *false*: For example, consider $F = \mathbb{Q}(\sqrt{2})$. Then conjugation (i.e., $\psi(a + b\sqrt{2}) = a - b\sqrt{2}$) is an automorphism of F, so if we assume that $\varphi : F \to \mathbb{C}$ is a homomorphism, then $\varphi \circ \psi : F \to \mathbb{C}$ is also a homomorphism. Therefore φ is not unique.

d. Given an algebraic extension $F/\mathbb{Q}$, there is a homomorphism (not necessarily unique) $F \to \mathbb{C}$ of fields. This is *true*.

e. There is an algebraically closed field of characteristic 2. This is *false*: Consider $f \in \mathbb{F}_2[x]$ where $f(x) = 1 + x + x^2$. Then $f(0) = 1$ and $f(1) = 1 + 1 + 1 = 1 + 0 = 1$, so f has a root that is not in $\mathbb{F}_2$.

5. Let F be a stem field for the irreducible polynomial $x^6 - 2 \in \mathbb{Q}[x]$. How many homomorphisms of fields $F \to \mathbb{R}$ are there?

Let $\alpha = \sqrt[6]{2}$ and $j = e^{\imath\pi/3}$, a primitive 6^{th} root of unity. Then the roots of $x^6 - 2$ are $r_1 = \alpha, r_2 = j\alpha, r_3 = j^2\alpha, r_4 = j^3\alpha = -\alpha, r_5 = j^4\alpha = -j\alpha, r_6 = j^5\alpha = -j^2\alpha$. Now for any stem field $F = \mathbb{Q}(r)$ where r is some root of $x^6 - 2$, we can define a homomorphism $f_n : F \to \mathbb{R}$ by $f_n(r) = r_n$ if $r_n \in \mathbb{R}$ ($f_n|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$). We see immediately that only $r_1 = \alpha$ and $r_4 = -\alpha$ are real numbers, so there are only *two* field homomorphisms from F into $\mathbb{R}$.

6. Let F be a stem field for the irreducible polynomial $x^6 - 2 \in \mathbb{Q}[x]$. How many homomorphisms of fields $F \to \mathbb{C}$ are there?

As above, but since every root of $x^6 - 2$ is in $\mathbb{C}$ (and they are all distinct!) we have *six* field homomorphisms from $\mathbb{F}$ into $\mathbb{C}$.

3 Lecture Notes: 07 Mar – 13 Mar

3.1 An example (of extension). Finite fields.

Here we formulate two corollaries on the theorem of extension of field homomorphisms.

Corollary 4. An algebraic closure of K is unique up to an isomorphism of K-algebras.

Corollary 5. Any algebraic extension of K embeds into the algebraic closure.

Example 9 (Example of extension of homomorphisms.)**.** Take $K = \mathbb{Q}$ and fix $\bar{\mathbb{Q}}$ (for example, take $\bar{\mathbb{Q}} \subset \mathbb{C}$ the "algebraic numbers," that is, all roots of polynomials in $\mathbb{Q}[x]$).

Let $L = \mathbb{Q}(\sqrt{2})$, but it is better to write $L = \mathbb{Q}[x]/\langle x^2 - 2\rangle$; and let α denote the class of x in L. L has two embeddings in $\bar{\mathbb{Q}}$: $\varphi_1 : \alpha \mapsto \sqrt{2}$ and $\varphi_2 : \alpha \mapsto -\sqrt{2}$ (each embedding is the identity when restricted to $\mathbb{Q}$).

Now consider $M = \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}[x]/\langle y^4 - 2\rangle$, with β denoting the class of y in M. M has four embeddings in $\bar{\mathbb{Q}}$: β can go to $\pm\sqrt[4]{2}, \pm\imath\sqrt[4]{2}$. Now $\psi_1 : \beta \mapsto \sqrt[4]{2}$ and $\psi_2 : \beta \mapsto -\sqrt[4]{2}$ extend φ_1: indeed, M is an extension of L, with $M = L[y]/\langle y^2 - \alpha\rangle, \varphi_1 : \alpha \mapsto \sqrt{2}$. Similarly $\psi_3 : \beta \mapsto \imath\sqrt[4]{2}$ and $\psi_4 : \beta \mapsto -\imath\sqrt[4]{2}$ extend φ_2, since $\pm\imath\sqrt[4]{2}$ are the square roots of $-\sqrt{2}$.

3.1.1 Finite fields.

We have seen that K a finite field necessarily means that K has characteristic p for some prime p; K is a finite extension over $\mathbb{F}_p$; if $n = [K : \mathbb{F}_p]$ then $|K| = p^n$. The usual notation is $K = \mathbb{F}_{p^n}$.

There are natural questions to ask: namely, whether it exists, and whether it is unique. We will shortly prove a theorem which answers these; but first, a remark about fields of characteristic p.

Remark 5. If K is a field of characteristic p, then $F_p : K \to K, x \mapsto x^p$ is a field homomorphism: $(x + y)^p = x^p + y^p, (xy)^p = x^p y^p$. This special mapping is called the "Frobenius homomorphism." Likewise, $F_{p^n} : x \mapsto x^{p^n}$ is also a field homomorphism—this is just a power of the Frobenius map.

Theorem 7. *Fix an algebraic closure $\mathbb{F}_p \subset \bar{\mathbb{F}}_p$. The splitting field of $x^{p^n} - x$ has p^n elements; conversely, any field of p^n elements is a splitting field of $x^{p^n} - x$. Moreover, there is a* unique *subextension of $\bar{\mathbb{F}}_p$ consisting of p^n elements.*

Proof. We have seen that $F_{p^n} : x \mapsto x^{p^n}$ is a homomorphism of fields. Then it follows that $\{x : F_{p^n}(x) = x\}$ is a subfield containing $\mathbb{F}_p$. But these are exactly the roots of $x^{p^n} - x = Q_n(x)$; this subfield is a splitting field of Q_n. Since Q_n does not have multiple roots (this can be seen, for

instance, by verifying that $\gcd(Q_n, Q_n') = 1$ as $Q_n' \equiv 1$), we have that there are p^n roots. Hence the splitting field of Q_n is exactly the field of roots of Q_n, and this field has p^n elements.

Conversely, let $|K| = p^n$ and $\alpha \in K$. Then $\alpha^{p^n-1} = 1$ provided $\alpha \neq 0$. Indeed, the multiplicative group of K, $K^\times$, has cardinality $p^n - 1$. So α is a root of $x^{p^n} - x$, and 0 is also a root. Hence K consists of roots of Q_n; the uniqueness of the subextension (of the image of the embedding) follows. ■

3.2 Properties of finite fields.

Now we formulate and prove another few properties of finite fields; these are very much in the spirit of the previous theorem.

Theorem 8. *$\mathbb{F}_{p^n} \supset F_{p^d}$ if and only if $d|n$.*

Proof. The "only if" direction rests on the multiplicativity of degrees in towers. We see that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}][\mathbb{F}_{p^d} : \mathbb{F}_p]$; substituting in the respective degrees, we see that $n = [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]d$, so $d|n$.

Conversely, suppose that $d|n$. Then if $x^{p^d} = x$, also $x^{p^n} = x$. Therefore $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. ■

Theorem 9. *$\mathbb{F}_{p^n}$ is a stem field and a splitting field of any irreducible polynomial $P \in \mathbb{F}_p[x]$ of degree n.*

Proof. The part about being a stem field is clear; indeed, a stem field of P has degree n over $\mathbb{F}_p$; this is $\mathbb{F}_{p^n}$. Now let α be a root of P. If $\alpha \in \mathbb{F}_{p^n}$, then $Q_n(\alpha) = 0$; hence P divides Q_n and so P splits in $\mathbb{F}_{p^n}$. ■

This has a simple corollary:

Corollary 6. $Q_n = \prod_{d|n} \prod_{P \text{ irred. monic of degree } d} P$.

Proof. We have already seen why: all such P divide Q_n (since the stem field is $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$). Then $\prod_{d|n} \prod_{P \text{ irred. monic of degree } d} P$ divides Q_n. Now Q_n has no multiple roots, so there are also no multiple factors, either; what remains to prove is that there are no other irreducible factors of Q_n.

Let R be an irreducible factor of Q_n. If α is a root of R, $Q_n(\alpha) = 0$, so $\mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$, which means that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$ where $d|n$. Hence $\deg R|n$, so there are no other irreducible factors. ■

3.3 Multiplicative group and automorphism group of a finite field.

Our next goal is a familiar theorem: the theorem saying that the multiplicative group of a finite field is cyclic. To make it instructive, we will prove it in a slightly more general version.

Theorem 10. *Let K be a field, and G a finite subgroup of $K^\times$. Then G is cyclic.*

Proof. The idea is to compare G and $\mathbb{Z}/n\mathbb{Z}$, where $n = |G|$. Let $\psi(d)$ denote the number of elements of order d in G. We now need to prove that $\psi(n) \neq 0$. We know that $n = \sum \psi(d)$. Denote by $\varphi(d)$ the number of elements of order d in $\mathbb{Z}/n\mathbb{Z}$; but as this is a cyclic group, it contains a single (cylic) subgroup of order d for each $d|n$. Namely, it contains the one generated by n/d. So $\varphi(d)$ gives the number of generators of $\mathbb{Z}/d\mathbb{Z}$; this is well known to be the number of numbers between 1 and $d-1$ which are prime to d. We know that $\varphi(n) \neq 0$. Now we claim that either $\psi(d) = 0$, or $\psi(d) = \varphi(d)$. This is sufficient, since $\sum \varphi(d) = \sum \psi(d) = n$. ■

Proof of claim. If there is no element of order d, then $\psi(d) = 0$; if there is one element x of order d in G, then x is a root of the polynomial $x^d - 1$. If you look at all the roots of such a polynomial, you see that they form a cyclic subgroup of G. So G, as well as $\mathbb{Z}/n\mathbb{Z}$, has a single (cyclic) subgroup of order d, or no such subgroup at all. (So far we know that $\mathbb{Z}/n\mathbb{Z}$ has such a subgroup for *any* d which divides n; with G this is not necessarily true *a priori*.)

If $\psi(d) \neq 0$ then there is such a subgroup, and the number of elements of order d, $\psi(d)$, is the number of generators of that subgroup; that is, whenever ψ is nonzero, it is equal to φ. Hence $\psi(d) \leq \varphi(d)$, but since $\sum \psi(d) = \sum \varphi(d)$ we must have $\psi(d) = \varphi(d)$. In particular, $\psi(n) \neq 0$. ■

Corollary 7. If K is an extension of $\mathbb{F}_p$ of degree n, then there exists α such that $K = \mathbb{F}_p(\alpha)$.

One might object and say that this has already been shown, as we have seen that $\mathbb{F}_{p^n}$ is a stem field of any irreducible polynomial of degree n. But this corollary is actually stronger, as we did not guarantee that such polynomials actually existed!

Corollary (contd.). In particular, there exists an irreducible polynomial of degree n over $\mathbb{F}_p$.

Proof. Since we know that $K^\times$ is cyclic, it suffices to take α to be a generator. ■

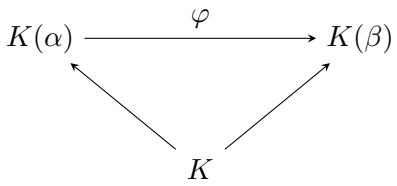
Corollary 8. The group $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic, generated by the Frobenius map $F : x \mapsto x^p$.

Proof. Of course, $x^{p^n} = x$ for any $x \in \mathbb{F}_{p^n}$ as we have seen, so $F^n = \mathrm{id}$. On the other hand, the order of F is exactly n, since if $m < n$ then F^m is not the identity (for instance, since $x^{p^m} - x = 0$ has

only p^m roots, and $p^m < p^n$). Finally, $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, where α is a root of an irreducible polynomial P of degree n. This α goes to another root of P under an automorphism, so $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq n$. Then the cardinality is in fact n, and the group is cyclic, generated by F. ■

3.4 Separable elements.

Our next topic is **separability**. We would like to say that a splitting field E of an irreducible polynomial P "has many automorphisms." By this we mean that if α, β are roots of P, and $E \supset K(\alpha)$ and $E \supset K(\beta)$, then there exists a homomorphism



such that φ extends to an automorphism of E.

There is one problem about this: is it true that an irreducible polynomial of degree n has "many" (that is, n) roots? The answer is yes, if K has characteristic 0; but this not always true if K has prime characteristic! P has multiple roots if and only if $\gcd(P, P') \neq 1$. In characteristic-0, this is never the case when P is irreducible ($\deg P' < \deg P$, and $P' \neq 0$ when P is non-constant, so P doesn't divide P'). In characteristic-p, P' can vanish, and then $\gcd(P, P') = P$. How can P' vanish? This happens exactly when P is a polynomial in x^p; that is to say, $P = \sum a_i x^i$ with $a_i \neq 0$ only if $p|i$.

Take $r = \max h : P$ is a polynomial in x^{p^h}, that is, $a_i = 0$ whenever p^h does not divide i. Then we can write $P(x) = Q(x^{p^r})$, in which case $Q' \neq 0$.

Proposition 8. *In particular,* $\gcd(Q, Q') = 1$ *and* Q *does not have multiple roots. Additionally, all roots of* P *have multiplicity* p^r*.*

Proof. If λ is a root of P, then $P = (x - \lambda)R$. Then $\mu = \lambda^{p^r}$ is a root of Q, so $Q(y) = (y - \lambda^{p^r})S$ where λ is not a root of S. Now set $y = x^{p^r}$, so $P(x) = (x^{p^r} - \lambda^{p^r})S(x^{p^r})$; this is just $(x - \lambda)^{p^r}$, and λ is not a root of $S(x^{p^r})$. Hence the multiplicity of λ is p^r. ■

Definition 11. Let $P \in K[x]$ be irreducible. Then P is called **separable** if $\gcd(P, P') = 1$. The **separable degree** of P, denoted $d_{sep}(P)$, is defined as $\deg Q$ as above. The **degree of insepa-**

rability, denoted $d_i(P)$ is defined as $\deg P / \deg Q$, which is p^r. P is called **purely inseparable** $\deg P = d_i(P)$—then $P(x) = x^{p^r} - a$.

Definition 12. Let L be an algebraic extension of K. An element $\alpha \in L$ is called **separable over** K or **purely inseparable over** K if its minimal polynomial, $P_{\min}(\alpha, K)$, has this property.

Proposition 9. *If α is separable over K, then $\left|\mathrm{Hom}_K(K(\alpha), \bar{K})\right| = \deg P_{\min}(\alpha, K)$. (In general: $\left|\mathrm{Hom}_K(K(\alpha), \bar{K})\right| = d_{\mathrm{sep}} P_{\min}(\alpha, K)$.)*

Proof. The proof is obvious, because the separable degree is just the number of distinct roots of P, so we can send alpha to any one of those roots. ■

3.5 Separable degree, separable extensions.

We can generalize this property to fields which are not necessarily given as $K(\alpha)$.

Definition 13. Take L to be an arbitrary finite extension of K. Define the **separable degree of** L **over** K, $[L : K]_{\mathrm{sep}}$, to be $[L : K]_{\mathrm{sep}} = \left|\hom KL, \bar{K}\right|$. (If $L = K(\alpha)$ this is just the number of distinct roots of $P_{\min}(\alpha, K)$.) We say that L is **separable** over K if $[L : K]_{\mathrm{sep}} = [L : K]$. Also, the **degree of inseparability** can be defined as $[L : K]_i = [L : K]/[L : K]_{\mathrm{sep}}$ (but this won't be very important going forward).

Theorem 11. *(1) Separable degree is multiplicative: if $K \subset L \subset M$, then $[M : K]_{\mathrm{sep}} = [M : L]_{\mathrm{sep}}[L : K]_{\mathrm{sep}}$; M is separable over K if and only if M is separable over L and L is separable over K.*

(2) The following are equivalent: (i) L is separable over K; (ii) any element $\alpha \in L$ is separable over K; (iii) $L = K(\alpha_1, \ldots, \alpha_n)$ with α_j separable over K; (iv) $L = K(\alpha_1, \ldots, \alpha_n)$, with each α_j separable over $K(\alpha_1, \ldots, \alpha_{j-1})$.

Remark 6. The same result holds when we replace "separable" by "purely inseparable."

Proof of (1). We know that any homomorphism $\varphi : L \to \bar{K}$ extends to $\tilde{\varphi} : M \to \bar{K}$; this is the extension theorem. In fact, there are exactly $[M : L]_{\mathrm{sep}}$ ways to do this, since given φ, one considers $\bar{K}$ as $\bar{L}$. Thus we have $[M : K]_{\mathrm{sep}} = [L : K]_{\mathrm{sep}}[M : L]_{\mathrm{sep}}$. Equivalence of separability is just the fact that $[E : K]_{\mathrm{sep}} \leq [E : K]$ for any extension E. The last fact is proved by induction, using the fact that this is true for $E = K(\alpha)$. ■

Proof of (2). (i) $\Rightarrow$ (ii): This is a consequence of part (1), which implies that any subextension $K(\alpha)$ of a separable extension L is itself separable.

(ii) $\Rightarrow$ (iii): This is obvious, as separability of any element implies that all the generators are separable.

(iii) $\Rightarrow$ (iv): This is clear because $P_{\min}(\alpha_j, K(\alpha_1, \ldots, \alpha_{j-1})$ divides $P_{\min}(\alpha_j, K)$. Then if $P_{\min}(\alpha_j, K)$ is seprable (has distinct roots), then so is its divisor.

(iv) $\Rightarrow$ (i): This can be proved by induction, as above. ■

One might ask: is the notion of separability defined for extensions which are not necessarily finite? Yes: if L over K is a not necessarily finite algebraic extension, we can define the **separable closure** $L^{\text{sep}} = \{x : x \text{ is separable over } K\}$. This L^{sep} is a subextension, and L is purely inseparable over L^{sep}.

Remark 7. (1) If K has characteristic 0, then any extension is separable.

(2) If K has characteristic p, then a purely inseparable extension has degree p^r. Always, $[L : K]_i = p^r$.

3.6 Perfect fields.

We have seen that fields of characteristic 0 have only separable extensions; but this is also true of *certain* fields of characteristic p. Such fields are called **perfect fields**. Let K be a field with characteristic p.

Definition 14. We say that K is **perfect** if $F : K \to K, x \mapsto x^p$ is surjective.

Example 10 (Perfect fields)**.** Any finite field is perfect, since an injective self-map of a finite set is surjective. Moreover, any algebraically closed field is perfect, since $x^p - a$ has a root α for any $a \in K$. In particular, $F(\alpha) = a$.

Example 11 (Non-perfect field)**.** Take $K = \mathbb{F}_p(x)$, the field of rational functions in one variable over $\mathbb{F}_p$. A typical element is of the form $f(x)/g(x)$, where $f, g \in \mathbb{F}_p[x]$. Then $\operatorname{Im} F = \mathbb{F}_p(x^p) \neq \mathbb{F}_p(x)$, since $x \notin F_p(x^p)$. Hence K is not perfect.

The following theorem illustrates why we care about perfect fields.

Theorem 12. *K is perfect if and only if all irreducible polynomials over K are separable—this means that all algebraic extensions of K are separable.*

Proof. First, suppose that K is perfect. Let $P \in K[x]$ and suppose that $P(x) = Q(x^{p^r}) = \sum a_i (x^{p^r})^i$. Since K is perfect, we can extract p^{th} roots of a_i's: there exists $b_i \in K$ such that $(b_i)^{p^r} = a_i$. Then $P = \left(\sum b_i x^i\right)^{p^r}$, which is not irreducible unless $r = 0$. Thus, irreducibility implies separability.

Conversely, if K is not perfect, then there exists $a \notin \operatorname{Im} F$. Then $x^{p^r} - a$ is irreducible: all roots in $\bar{K}$ are the same α with $\alpha^{p^r} = a$, and $\alpha^{p^{r-1}} \notin K$. We have already seen that in this case, the degree of $K[x]$ over K is exactly p^r. This completes the proof. ■

3.7 Week 3 Quiz

1. Which of the following are true?

The degree of a finite extension $K/\mathbb{F}_p$ is divisible by p. This claim is *false*: for example, take $\mathbb{F}_2[x]/(x^3+x+1)$ over $\mathbb{F}_2$. Since the polynomial has degree 3 the extension has order $2^3 = 8$; but the *degree* is 3 which is not divisible by 2.

The number of elements in a field extension $K/\mathbb{F}_p$ is equal to p^n for some n. This claim is *true*.

$\mathbb{F}_{p^2}$ can be embedded as a subfield of $\mathbb{F}_{p^3}$. This claim is *false* by Thm. 8: We can perform an embedding $\mathbb{F}_{p^d} \hookrightarrow \mathbb{F}_{p^n}$ only if $d|n$, and 2 does *not* divide 3.

$\mathbb{F}_{p^2}$ can be embedded as a subfield of $\mathbb{F}_{p^4}$. This claim is *true* by Thm. 8: Since 2 divides 4, we can perform the embedding.

Any two finite fields of the same order are isomorphic. This claim is *true*.

2. Which of the following are true?

A finite field of order p^n has a unique subfield of order p^m for every m dividing n. This is *true* by Thm. 8: For each m dividing n, the theorem implies that $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$.

An algebraic closure $\overline{\mathbb{F}_p}$ can contain many different subfields of order p^n for some n. This claim is *false* by Thm. 7: such a subfield will be unique.

For every n, there is an irreducible polynomial $P \in \mathbb{F}_p[x]$ of degree n This claim is *true* by Cor. 7 (to Thm. 10).

The group of automorphisms of a field F of order p^n has order $n!$. This claim is *false*: the group is cyclic so it has order p^n.

3. Which of the following are true?

It is possible for an irreducible polynomial in $\mathbb{Q}[x]$ to be inseparable (have multiple roots). This claim is *false*, because $\mathbb{Q}$ has characteristic 0 and therefore irreducibility implies separability.

Every irreducible polynomial over a finite field K is separable (has no multiple roots). This claim is *true*: see example 10.

The polynomial $x^p - t \in \mathbb{F}_p(t)[x]$ over the field of rational functions $\mathbb{F}_p(t)$ is separable. This claim is *false*: The derivative $P' = (d/dx)(x^p - t) = px^{p-1} = 0$, so $\gcd(P, P') = P \neq 1$. Therefore the polynomial is not separable.

The stem field $F_p(t^{1/p})$ for the polynomial $x^p - t$ has degree p over $\mathbb{F}_p(t)$ and is a splitting field for $x^p - t$. This claim is *true*: $\mathbb{F}_p(t^{1/p})$ is generated by $1, t^{1/p}, t^{2/p}, \ldots, t^{1-1/p}, t$ over $\mathbb{F}_p$, so it has degree p.

Define $\alpha = t^{1/p}$.

4. Which of the following are true?

3.8 Ungraded Assignment: February 21, 2016

Question 1. Let $F(x)/G(x) \in K(X)$ be a rational function over a field K. Show that the extension $K(F/G)/K(X)$ is algebraic and compute its degree.

Proof. ■

Question 2. Let L/K be an algebraic extension and $\varphi : L \to L$ a K-algebra homomorphism. Show that φ is always an isomorphism. Give a counterexample when L/K is not algebraic.

Proof. ■

Counterexample when L/K is not algebraic. ■

Question 3. Let m, n be square-free integers with $m \neq n$ and $m, n \neq 1$. Show that $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$. Find the degree of $\sqrt{m} + \sqrt{n}$ over $\mathbb{Q}$ and compute its minimal polynomial.

Proof. ■

Question 4. Show that $x^4 + 1$ is reducible modulo every prime p but irreducible over $\mathbb{Z}$. (Hint: $p = 2$ is easy and for $p \neq 2$, consider the group of units in $\mathbb{F}_{p^2}$.)

Proof. ■

Question 5. Show that $x^p - x - 1$ is irreducible over $\mathbb{F}_p$. (Hint: Show it has has no root in $\mathbb{F}_p$ and show that if α is a root in some extension, the nall other roots are of the form $\alpha + a$ for $a \in \mathbb{F}_p$.)

Proof. ■

Question 6. What is the degree of the splitting field of $x^5 - 7$ over $\mathbb{Q}$?

Solution. ■

Question 7. What is the degree of the splitting field of $x^6 + x^3 + 1$ over $\mathbb{F}_p$ for (i) $p \equiv 1 \bmod 9$, (ii) $p \equiv 2 \bmod 9$, (iii) $p \equiv 7 \bmod 9$?

Proof. ■

4 Lecture Notes: 14 Mar – 20 Mar

We have been considering $[L : K]$ a finite field extension, and defined separability: If L is generated over K by a finite number of separable elements $\alpha_1, \ldots, \alpha_r$, then the number of homomorphisms over K from L to an algebraic closure $\bar{K}$ is equal to the degree of L over K. (In general, this number of homomorphisms is less than or equal to the degree.) We have called this number of homomorphisms the **separable degree** of L over K.

If $L = K(\alpha)$, this was clear, as the homomorphisms took α to the other roots of the minimal polynomial. In general, one can use induction and the multiplicativity of the degree (which is just linear algebra) and the number of homomorphisms (theorem on extension of homomorphisms). A **separable extension** was just that which had the right number of homomorphisms.

We will characterize separability in terms of **tensor products**. This is a general digression that does not have much to do with field extensions.

4.1 Definition of a tensor product.

Definition 15 (Tensor product of modules)**.** Let A be a ring, and M, N be A-modules. The **tensor product** of M and N over A, denoted $M \otimes_A N$, is another A-module together with an A-bilinear map $\varphi : M \times N \to M \otimes_A N$ with the following "universal property": If P is any A-module and $f : M \times N \to P$ is A-bilinear (i.e. for any m, n, the maps $f_m : N \to P, n \mapsto f(m, n)$ and $f_n : M \to P, m \mapsto f(m, n)$ are homomorphisms of A-modules) then there exists a unique homomorphism of A-modules $\tilde{f} : M \otimes_A N \to P$ such that $f = \tilde{f} \circ \varphi$.

This property characterizes the pair $(\varphi, M \otimes_A N)$. If $(\bar{\varphi}, \overline{M \otimes_A N})$ is another such pair, then by definition we have mutually inverse homomorphisms of A-modules between our tensor products $M \otimes_A N$ and $\overline{M \otimes_A N}$. So the uniqueness of tensor products follows directly from the definition, but of course the real question is: why does such a thing even exist?

We can give a construction as follows: Consider $\mathcal{E}$ the family of maps from $M \times N$ to A *as sets* which are zero almost everywhere, that is, outside of a finite set. (For example, delta-functions $\delta_{m,n} : M \times N \to A$, where $\delta_{m,n}(m, n) = 1$ and $\delta_{m,n}(m', n') = 0$ for all $(m', n') \neq (m, n)$.) This $\mathcal{E}$ is a **free** A-module with base $\delta_{m,n}$. Now, we have a map of sets $M \times N \to \mathcal{E}$ that sends $(m, n) \mapsto \delta_{m,n}$; this is not necessarily bilinear, but we can make it so. Take $\mathcal{F} \subset \mathcal{E}$ a submodule generated by

$$\delta_{m+m',n} - \delta_{m,n} - \delta_{m',n}, \delta_{m,n+n'} - \delta_{m,n} - \delta_{m,n'}, \delta_{am,n} - a\delta_{m,n}, \delta_{m,an} - a\delta_{m,n}$$

Now the *map to the quotient* $M \times N \to \mathcal{E}/\mathcal{F}$ is bilinear, and has the desired universal property.

4.2 Tensor product of modules.

If we have any bilinear map $M \times N \to P$, we can also define a map $\tilde{f} : \mathcal{E} \to P$ sending $\delta_{m,n} \mapsto f(m,n)$. When the map f is bilinear, then the map from $\mathcal{E} \to P$ must factor through the quotient $\mathcal{E}/\mathcal{F}$, and moreover is zero on $\mathcal{F}$! So we can complete the diagram with the bilinear map $M \times N \to \mathcal{E}/\mathcal{F}$. We also have uniqueness since the map $\mathcal{E} \to P$ is determined by the images of $\delta_{m,n}$. We can then call the map from $M \times N \to \mathcal{E}/\mathcal{F}$ φ, and identify $\mathcal{E}/\mathcal{F} = M \otimes_A N$.

The tensor product $M \otimes_A N$ is generated by the classes of $\delta_{m,n}$ modulo $\mathcal{F}$; we will denote them by $m \otimes n$.

Remark 8. The tensor product is not equal to $\{m \otimes n : m \in M, n \in N\}$; we can write any $x \in M \otimes_A N$ as a finite sum of symbols $\sum_{i=1}^{n} m_i \otimes n_i$ but we cannot reduce further.

We might ask, why haven't we simply *defined* the tensor product by this more explicit construction? Why are we talking about this "universal property"? It turns out that the proofs become easier when we use the universal property. For example, we want to show that $M \otimes_A N \simeq N \otimes_A M$. Indeed $M \times N \to N \otimes_A M$ where $(m,n) \mapsto n \otimes m$ is bilinear; therefore we have $\alpha : M \otimes_A N \to N \otimes_A M$. In the same way we obtain the inverse map in the other direction.

The same type of argument yields, for example, that $A \otimes_A M \simeq M$.

More seriously, we have seen that the tensor product is generated by those "little" tensor products: If M is generated by $\{e_i\}_{i=1}^{n}$ and N is generated by $\{\varepsilon_j\}_{j=1}^{m}$, then $M \otimes_A N$ is generated by $e_i \otimes \varepsilon_j$.

Proposition 10. *We can also prove that if $e_i, 1 \le i \le n$ is a* basis *of M and $\varepsilon_j, 1 \le j \le m$ is a basis of N (that is, both M and N are free modules over A), then $e_i \otimes \varepsilon_j, 1 \le i \le n, 1 \le j \le m$ is a basis of $M \otimes_A N$.*

Proof. This is easily shown with the universal property. Define a bilinear map $f_{i_0,j_0} : M \times N \to A$ sending $(\sum a_i e_i, \sum b_j \varepsilon_j)$ to $a_{i_0} b_{j_0}$. Since f_{i_0,j_0} is bilinear, it factors through the tensor product $\tilde{f}_{i_0,j_0} : M \otimes_A N \to A$, where $\tilde{f}_{i_0,j_0}$ sends $e_{i_0} \otimes \varepsilon_{j_0}$ to 1 and all other $e_i \otimes \varepsilon_j$ to 0. So if $\sum \alpha_{ij} e_i \otimes \varepsilon_j = 0$, then applying $\tilde{f}_{i_0,j_0}$ we see that $\alpha_{i_0 j_0} = 0$. Doing this for all i_0, j_0, we conclude that all coefficients are zero. ∎

Example 12. In particular, the tensor product of K-vector spaces with bases $\{e_i\}$, $\{\varepsilon_j\}$ is a K-vector space with a base $e_i \otimes \varepsilon_j$. One usually introduces these symbols formally and builds a vector space on top; however, in general it's better to use the universal property.

4.3 Base change.

We also have other (more or less) elementary properties of the tensor product.

Example 13. For example, we have a sort of associativity: $(M_1 \otimes_A M_2) \otimes_A M_3 \simeq M_1 \otimes_A (M_2 \otimes_A M_3)$. To prove this, we introduce $M_1 \otimes_A M_2 \otimes_A M_3$ as a universal object for *trilinear* maps, and then show that both parts are isomorphic to this object.

Definition 16 (Base change)**.** Let A be a ring, B be an A-algebra, M and A-module, and N a B-module. We can make N into an A-module, by "forgetting" the B-module structure. We can "make" M into a B-module by considering $B \otimes_A M$. Introduce the B-module structure on $B \otimes_A M$ by setting $b \cdot (b' \otimes m) = bb' \otimes m$.

This may seem sophisticated, but we have certainly encountered some examples before.

Example 14. We can "make" $\mathbb{C}^n$ into $\mathbb{R}^{2n}$ by forgetting the complex multiplication: if $\mathbb{C}^n$ has basis $\{e_i\}$, we just forget that we can multiply by the imaginary unit, and so we give $\mathbb{R}^{2n}$ the basis $\{e_1, \ldots, e_n, v_1, \ldots, v_n\}$, where $v_i = \imath e_i$.

If we want to "complexify" $\mathbb{R}^{2n}$, we can consider $\mathbb{C} \otimes \mathbb{R}^{2n} = \mathbb{C}^{2n}$ with basis $\{e_1, \ldots, e_n, v_1, \ldots, v_n\}$ (forgetting that $v_i = \imath e_i$)—more precisely, one should write $1 \otimes e_1, \ldots, 1 \otimes e_n, 1 \otimes v_1, \ldots, 1 \otimes v_n$.

One can go the other way. If $\mathbb{R}^n$ has basis $e_1, \ldots, e_n$, then we can make it into a complex vector space $\mathbb{C}^n = C \otimes^n_{\mathbb{R}}$ with a $\mathbb{C}$-basis $1 \otimes e_i$, and make *that* into $\mathbb{R}^{2n}$ by forgetting the complex structure, with an $\mathbb{R}$-basis $1 \otimes e_1, \ldots, 1 \otimes e_n, \imath \otimes e_1, \ldots, \imath \otimes e_n$.

In general, if M is a fee A-module with a base $e_1, \ldots, e_n$, then $B \otimes_A M$ is a free B-module with base $1 \otimes e_1, \ldots, 1 \otimes e_n$. We also have maps $M \to B \otimes_A M, m \mapsto 1 \otimes m$ of A-modules; and maps $B \otimes_A N \to N, b \otimes n \mapsto bn$ of A-modules. The proof of this story about the bases is the same as what we've seen before in Proposition 1: we construct certain bilinear maps that factor over the tensor product, which implies that certain families are linearly independent.

Theorem 13 (Base change)**.** *The A-homomorphisms between M and N are in bijection with the B-homomorphisms between $B \otimes_A M$ and N. (Alternatively, you can say that* $\mathrm{Hom}_A(M, N) \simeq \mathrm{Hom}_B(B \otimes_A M, N)$ *as groups, etc.)*

Proof. If I have a homomorphism $f : B \otimes_A M \to N$, we can compose it with the embedding $\alpha : M \to B \otimes_A M$, so in the one direction we have $f \mapsto f \circ \alpha$. In the other direction, if we have $g : M \to N$, then we can "tensor it" with B to obtain $id \otimes g : B \otimes_A M \to B \otimes_A N$. Then we compose this map with $\mu : B \otimes_A N \to B$ sending $b \otimes n \mapsto bn$, so we have $g \mapsto \mu \circ (id \otimes g)$. It's easy to check that the maps are mutually inverse. ∎

4.4 Examples. Tensor product of algebras.

Here we give an example of a base change.

Proposition 11. *Let $I \subset A$ be an ideal (so the ring in question will be A/I). Then $A/I \otimes_A M \simeq M/IM$, where IM is a sub-module of M.*

Proof. Define $M \xrightarrow{\alpha} A/I \otimes M$ by $m \mapsto 1 \otimes m$. This sends IM to zero. That is, if we have im where $i \in I$, then $im \mapsto 1 \otimes im$, but the tensor product is over A, and so everything is A-linear: $1 \otimes im = i \otimes m = 0 \otimes m = 0$. Hence α induces a map $M/IM \xrightarrow{\bar{\alpha}} A/I \otimes_A M$.

Now, in the other direction, we apply the Base Change Theorem: consider the projection $M \to M/IM$ of A-modules. Setting $B = A/I$, we can then obtain a map $B \otimes_A M \to M/IM$ of A-modules. We can again check that this map is in fact the inverse of $\bar{\alpha}$. ■

Now we consider some examples.

Example 15 (Base-changing rings of integers)**.** Consider $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$. Then we can think of this as a base change from $\mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$, and so this is isomorphic to $(\mathbb{Z}/3\mathbb{Z})/((2) \cdot \mathbb{Z}/3\mathbb{Z})$. But $(2) \cdot \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$, and so the the quotient is 0!

Example 16 (Base-changing polynomial rings)**.** Changing the base of a polynomial ring from A to B just gives a polynomial ring over B: $B \otimes_A A[x] \simeq B[x]$

Example 17 (Base-changing quotient rings)**.** As you might expect from the previous example, $B \otimes_A A[x]/(P) \simeq B[x]/(P)$, but on the RHS (P) is now the ideal generated by P in $B[x]$.

Now, given two A-algebras B and C, and $\alpha : A \to B$ (respectively $\beta : A \to C$) defining the A-algebra structure on B (respectively C), we can define a new A-algebra $B \otimes_A C$. This is a ring with respect to $(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'$.

In fact, this has the following universal property: if $\varphi : B \to B \otimes_A C, b \mapsto b \otimes 1$ and $\psi : C \to B \otimes_A C, c \mapsto 1 \otimes c$, and D is any A-algebra, we have that $\mathrm{Hom}_A(B \otimes_C, D)$ is in bijection with $\mathrm{Hom}_A(()B, D) \times \mathrm{Hom}_A(C, D)$. If we have $h : B \otimes_A C \to D$, this is the same thing as having $B \xrightarrow{f} D$ and $C \xrightarrow{g} D$ such that $h = f \times g$ (and the diagram commutes): $h \mapsto (h \circ \varphi, h \circ \psi$, and conversely, given f, g, we can define $h(b \otimes c) = f(b) \cdot g(c)$.

The main point for us is that the tensor product of two A-algebras is itself an A-algebra by componentwise multiplication.

Example 18. Consider $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Then we have

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \otimes \mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}[x]/(x^2+1)$$

and then by the Chinese Remainder Theorem (see below) we conclude that $\mathbb{C}[x]/(x^2+1) \simeq \mathbb{C}[x]/(x+\imath) \times \mathbb{C}[x]/(x-\imath)$, which is then isomorphic to $\mathbb{C} \times \mathbb{C}$. We can then conclude that this tensor product is *not* a field, in particular because it has zero-divisors. These can be seen, for example, by noticing that the class $\overline{x+\imath}$ is a zero-divisor, which can be represented by $1 \otimes \bar{x} + \imath \otimes \bar{1}$—then in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ this is just $1 \otimes \imath + \imath \otimes 1 = 0$.

4.5 Relatively prime ideals. Chinese Remainder Theorem.

Now we explore the structure of a finite algebra A over a field K. (That is, a finite-dimensional vector space.) First, we recall the Chinese remainder theorem.

Definition 17. Let A be a ring with I, J ideals. We say that I and J are **relatively prime** if $I + J = A$.

Lemma 4. *(1) If I, J are relatively prime then $IJ = I \cap J$; (2) If $I_1, \ldots, I_k$ are relatively prime to J, then so is $\bigcap_{j=1}^{k} I_j$; (3) If I, J are relatively prime then so are I^k, J^l for any k, l.*

Proof of lemma. (1) That $IJ \subset I \cap J$ is clear; this is just by definition. Now if I and J are relatively prime, then $1 = i + j$ for some $i \in I$ and $j \in J$. Hence for any $x \in I \cap J$ we have $x = xi + xj$, and both $xi, xj \in IJ$, so $x \in IJ$.

(2) Suppose that $k = 2$; the general case is similar. Then we have $1 = i_1 + j_1 = i_2 + j_2$ where $i_1 \in I_1$, $i_2 \in I_2$, and $j_1, j_2 \in J$. Now write $1 = (i_1 + j_1)(i_2 + j_2) = i_1 i_2 + j_1 i_2 + j_2 i_1 + j_1 j_2$. We see that $i_1 i_2 \in I_1 I_2$, and $j_1 i_2 + j_2 i_1 + j_1 j_2 \in J$, which is what we want to prove.

Finally, (3) follows from (2) by induction. ■

Theorem 14 (Chinese remainder)**.** *Let $I_1, \ldots, I_n$ be ideals of A, and $\pi : A \mapsto A/I_1 \times \cdots \times A/I_n$, $a \mapsto (a \bmod I_1, \ldots, a \bmod I_n)$. (So $\operatorname{Ker} \pi = I_1 \cap \ldots \cap I_n$). Then π is surjective if and only if $I_1, \ldots, I_n$ are pairwise relatively prime. In this case $A/\bigcap I_k \simeq A/\prod I_k \simeq \prod (A/I_k)$.*

Proof. Suppose π is surjective. Then there exists a_i such that $\pi(a_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$, that is, 1 in the i^{th} place and all other entries 0. This means $a_i \in I_j$ for some $j \neq i$, and $1 - a_i \in I_i$. Hence I_i is relatively prime to any I_j, since $1 = (1 - a_i) + a_i$.

Conversely, suppose that all the ideals are (pairwise) relatively prime; then I_i is relatively prime to $\prod_{j\neq i} I_j$. Hence there exist $x_i \in I_i, y_i \in \prod_{j\neq i} I_j$ such that $x_i + y_i = 1$. Such an element y_i maps to $(0,\ldots,0,1,0,\ldots,0)$ with the 1 in the i^{th} place. Then $\sum_{i=1}^n b_i y_i \mapsto (b_1,\ldots,b_n)$ for all b_i, and so π is surjective. This proves the theorem. ■

Now consider A a finite algebra over K. Before proving a general theorem on the structure of A, we state proposition.

Proposition 12. *(1) If A is an integral domain, then A is a field;*

(2) (rephrasing) Any prime ideal of A is maximal.

Proof. It suffices to prove the first part, as the second part is just a consequence of definitions: in fact, a quotient over a prime ideal is an integral domain, and a quotient over a maximal ideal is a field.

Suppose now that A is an integral domain: that is, for any $a \in A$, the multiplication by a is injective. But A is a finite dimensional K-vector space, so this implies that multiplication by a is an isomorphism. In particular it is surjective, so there exists a b such that $b \cdot a = 1$. Therefore A is a field, since 1 has a pre-image, b. ■

4.6 Structure of finite algebras over a field. Examples.

Theorem 15 (Structure of finite K-algebras.)**.** *Let A be a finite K-algebra (that is, A is a finite dimensional K-vector space). Then:*

(1) There are only finitely many maximal ideals $\mathfrak{m}_1,\ldots,\mathfrak{m}_r$ in A;

(2) Let $J = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r = \mathfrak{m}_1 \times \cdots \times \mathfrak{m}_r$ (since they are relatively prime). Then $J^n = 0$ for some n;

(3) $A \simeq A/\mathfrak{m}_1^{n_1} \times \cdots A/\mathfrak{m}_r^{n_r}$ for some $n_1,\ldots,n_r$.

Proof. (1) Let $\mathfrak{m}_1,\ldots,\mathfrak{m}_i$ be maximal ideals. By the Chinese remainder theorem, we have $A/\mathfrak{m}_1\cdots\mathfrak{m}_i \simeq A/\mathfrak{m}_1 \times \cdots A/\mathfrak{m}_i$. Now $A/\mathfrak{m}_1\cdots\mathfrak{m}_i$ and any such $A/\mathfrak{m}_j$ are finite-dimensional K-vector spaces, and

$$\dim_K A \geq \dim_K A/\mathfrak{m}_1\cdots\mathfrak{m}_i = \sum_{j=1}^{i} \dim_K A/\mathfrak{m}_j \geq i$$

So the number of maximal ideals is at most $\dim_K A$; that is, there are only finitely many.

(2) J is also a finite dimensional vector space over K, and so are its powers. Now consider the decreasing sequence $J \supseteq J^2 \supseteq J^3 \ldots \supseteq J^k \supseteq \ldots$; the dimension is nonincreasing with each step. Hence the sequence must stabilize; for some n we must have $J^n = J^{n+1}$. We claim that $J^n = 0$. Indeed, if not, let $e_1, \ldots, e_s$ be a basis for J^n. As $J^n = J \cdot J^n$, we can write $e_i = \sum \lambda_{ij} e_j$ for some $\lambda_{ij} \in J$. If we consider the matrix $M = Id - \lambda_{ij}$ we have that

$$M \begin{pmatrix} e_1 \\ \vdots \\ e_s \end{pmatrix} = 0$$

This is just the same as the previous equation. Since M is a matrix over a ring and not over a field, this does not immediately mean that the e_i's are 0, but we can always find a matrix $\tilde{M}$ such that $\tilde{M}M = \det M \cdot Id$. Then $\det M \cdot (e_1, \ldots, e_s)^T = 0$, but $\det M = 1 + \lambda$ where $\lambda \in J$. Since $J = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r$, $\lambda \in \mathfrak{m}_i$ for all i, and so there is no i for which $1 + \lambda \in \mathfrak{m}_i$. This means that $1 + \lambda$ is invertible, and therefore $e_1 = \cdots = e_s = 0$, a contradiction.

(3) By part 2, we can find $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ such that $\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r} = 0$; we can, for example, take $n_i = n$ for all i. Then, by Chinese remainder theorem, since all the $\mathfrak{m}_i^{n_i}$ are pairwise relativel prime, we have

$$A/\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r} = A \simeq A/\mathfrak{m}_1^{n_1} \times \cdots \times A/\mathfrak{m}_r^{n_r}$$

This proves the theorem. ■

Remark 9. The n_i's are *not* uniquely determined; we could have taken all of them equal to n, but we can also write this identity with at least some n_i's different from n. For instance, let $A = K[x]/(x^2 \cdot (x+1)^3)$. Then $\mathfrak{m}_1 = (x), \mathfrak{m}_2 = (x+1)$, and $A \simeq A/\mathfrak{m}_1^2 \times A/\mathfrak{m}_2^3$, but also $A \simeq A/\mathfrak{m}_1^3 \times A/\mathfrak{m}_2^3$. The reason is very simple: in fact $\mathfrak{m}_1^2 = \mathfrak{m}_1^3$. In A, we have $(x)^2 \supset (x)^3$ but *also* $(x)^3 \supset (x)^2$; this is true in A but not in the polynomial ring, and the verification is left as an exercise.

Now we consider some examples.

Example 19. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$; $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. These algebras are products of fields; all $n_i = 1$ (in other words, we do not have nilpotents, so these are **reduced** algebras).

This is a general phenomenon: the presence of nilpotents is due to the *inseparability* of extensions.

4.7 Week 4 Quiz

1. Which of the following modules are non-zero?

a. $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/5\mathbb{Z}$**?** We use Proposition 11 with $I = (3)$ as our ideal. Hence

$$\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/5\mathbb{Z} \simeq (\mathbb{Z}/5\mathbb{Z})/((3) \cdot (\mathbb{Z}/5\mathbb{Z}))$$

But $(3) \cdot (\mathbb{Z}/5\mathbb{Z}) = \mathbb{Z}/5\mathbb{Z}$ since $\gcd(3, 5) = 1$. Therefore the tensor product is zero.

b. $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/9\mathbb{Z}$**?** Again Prop. 11 yields $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/9\mathbb{Z} \simeq (\mathbb{Z}/9\mathbb{Z})/((3) \cdot (\mathbb{Z}/9\mathbb{Z}))$, but this time $(3) \cdot (\mathbb{Z}/9\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$, so the tensor product is isomorphic to $(\mathbb{Z}/9\mathbb{Z})/(\mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$.

c. $\mathbb{Q}[x]/(x-1) \otimes_{\mathbb{Q}} \mathbb{Q}[x]/(x+1)$**?** Note that we cannot use Prop. 11 here, since $(x-1)$ is not an ideal in $\mathbb{Q}$.

d. $\mathbb{Q}[x]/(x-1) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x+1)$**?** Here we *can* use Prop. 11, as $(x-1)$ is an ideal in $\mathbb{Q}[x]$. Hence

$$\mathbb{Q}[x]/(x-1) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x+1) \simeq (\mathbb{Q}[x]/(x+1))/((x-1) \cdot (\mathbb{Q}[x]/(x+1)))$$

But $x-1$ and $x+1$ are relatively prime, since

$$\left(\frac{1}{2}\right)(x+1) + \left(\frac{-1}{2}\right)(x-1) = \frac{x}{2} + \frac{1}{2} - \frac{x}{2} + \frac{1}{2} = 1$$

Therefore $(x-1) \cdot (\mathbb{Q}[x]/(x+1)) \simeq (\mathbb{Q}[x]/(x+1))$ and so the tensor product is zero.

2. Consider a commutative ring A and an unknown element $x \in A$. Which of the following systems of congruences has a solution for any choice of $a, b \in A$? (Hint: Chinese remainder theorem.)

We want the two moduli to be relatively prime.

3. Which of the following algebras are products of fields (maybe with only one factor)?

4. Which of the following statements are true?

5. Let k be a field, A a k-algebra of dimension 2. Choose $x \in A$, $x \notin k \subset A$. Then A is generated by 1 and x and so there is an isomorphism of algebras $k[x]/(x^2 + ax + b) \simeq A$ for some $a, b \in k$. Which of the following statements are true?

Let $L = k[x]/(x^2 + ax + b)$. Since $[A : k] = 2$, we need $[L : k] = 2$, that is, we need the polynomial $x^2 + ax + b$ to have two distinct roots in k.

Case 5a: $k = \mathbb{Q}$.

Claim: There are infinitely many *non-isomorphic possibilities for A.* ■

Case 5b: $k = \mathbb{F}_p$.

Claim: There are xxx *possibilities for A, up to isomorphism.* ■

Case 5c: k is algebraically closed.

Claim: There are two *possibilities for A, up to isomorphism.* ■

5 Lecture Notes: 21 Mar – 28 Mar

5.1 Structure of finite K-algebras, examples (cont'd)

Last time we have seen that a finite algebra over a field was a product of certain quotients by powers of maximal ideals. Such a k-algebra A has only finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ and is isomorphic to $A/\mathfrak{m}_1^{k_1} \times \cdots A/\mathfrak{m}_r^{k_r}$; this is a sort of "generalized form" of the Chinese Remainder Theorem. For example, if $A = K[x]/(F)$ where F is a (not necessarily reducible) polynomial, we can decompose $F = P_1^{k_1} \cdots P_r^{k_r}$; then by the Chinese Remainder theorem we have

$$A \simeq K[x]/(P_1^{k_1}) \times \cdots \times K[x]/(P_r^{k_r})$$

Here, every such factor is $A/\mathfrak{m}_\mathfrak{i}^{k_i}$, where $\mathfrak{m}_\mathfrak{i}$ is the ideal generated by $P_i \pmod F$. So now let us give a couple of definition.

Definition 18. An algebra A is called **reduced** if it has no nilpotents (recall that $x \in A$ is nilpotent if $x \neq 0$ but $x^k = 0$ for some k). This is the same as saying that, in the decomposition $A/\mathfrak{m}_1^{k_1} \times \cdots A/\mathfrak{m}_r^{k_r}$, all the k_i are equal to 1. This is the same as saying that A is a product of fields $A/\mathfrak{m}_i$.

Definition 19. An algebra A is called **local** if it has only one maximal ideal, so $A \simeq A/\mathfrak{m}^k$. (Here there are lots of nilpotents; all elements of $\mathfrak{m}$ are nilpotents, so each $x \in A$ is a unit, zero, or nilpotent.)

These definitions extend to non-finite extensions, but we lose the structure theorems; hence (e.g.) we cannot say that every element in a non-finite local extension is a unit, zero, or nilpotent.

Last time we saw that $\mathbb{C} \otimes_\mathbb{R} \mathbb{C}$, $\mathbb{Q}(\sqrt{2} \otimes_\mathbb{Q} \mathbb{Q}(\imath)$, etc. were reduced: $\mathbb{C} \otimes_\mathbb{R} \mathbb{C} = \mathbb{C} \times \mathbb{C}$, $\mathbb{Q}(\sqrt{2} \otimes_\mathbb{Q} \mathbb{Q}(\imath)$ is a field, and so on. If we start producing similar examples, mostly they are reduced. Why? The presence of nilpotents reflects inseparability.

Let K be a field of characteristic p, and consider the field of rational functions $K(X)$ as an extension of $K(X^p)$, which we denote $K(Y)$ for simplicity of notation. Now find the tensor product $K(X) \otimes_{K(Y)} K(X)$. This is the same thing as $K(X) \otimes_{K(Y)} K[T]/(T^p - Y) \simeq K(X)[T]/T^p - X^p \simeq K(X)[T]/(T - X)^p$. This ring has a lot of nilpotents! For instance, $T - X$, since $K(X)$ is a purely inseparable extension of $K(Y)$.

5.2 Separability and base change.

So, what is the reason for such a mysterious connection between the presence of nilpotents and separability? Recall that separable extension L over a field K has a maximal possible number of homomorphisms into the algebraic closure; in fact, equal to the degree of L over K. This is clear, because if we have a polynomial with distinct roots then its stem field (for instance) has exactly this number of homomorphisms into the homomorphisms. If some roots coincide, then the number of homomorphisms diminishes. Now recall the base-change formula: If we have L, E extensions of K, with L finite over K, then $\mathrm{Hom}_K(L, E) \simeq \mathrm{Hom}_E(L \otimes_K E, E)$. Now $L \otimes_K E = A$ is a finite E-algebra, and so $A \simeq A/\mathfrak{m}_1^{k_1} \times \cdots \times A/\mathfrak{m}_r^{k_r}$. Now define A_{red} ("A-reduced") by $A_{\mathrm{red}} := A/\mathfrak{m}_1 \times \cdots A/\mathfrak{m}_r$. We see that $A_{\mathrm{red}} = A/\mathcal{N}(A)$, where $\mathcal{N}(A)$ is the ideal generated by the nilpotent elements of A. Then it is clear that if we look at the homomorphisms $\mathrm{Hom}_E(A, E)$, this is the same as the homomorphisms $\mathrm{Hom}_E(A_{\mathrm{red}}, E)$ since any homomorphism into a field must be zero on all nilpotents! Therefore we see that if there are nilpotents in the tensor product, then there is somehow "less space" for homomorphisms, giving us the following "slogan": "If A is not reduced, then $[A_{\mathrm{red}} : E] < [A : E]$, so the maximal number of homomorphisms is attained when A is reduced and all quotients $A/\mathfrak{m}_i \simeq E$." In general, the quotients $A/\mathfrak{m}_i$ are extensions of E. $A \simeq A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_r$ $\mathrm{Hom}_E(A/\mathfrak{m}_i, E) = \{0\}$ if $[A/\mathfrak{m}_i : E] > 1$, because an E-homomorphism of fields which are extensions of E must be injective.

Now let us take $E = \overline{K}$. Then $A/\mathfrak{m}_i \simeq E$ automatically since an algebraically closed field has no non-trivial finite extensions. We have $A = L \otimes_K \overline{K}$, $A_{\mathrm{red}} = \prod_{r\mathrm{times}} \overline{K}$ and $A = A_{\mathrm{red}}$ if and only if r is maximal, equal to $[L : K] = [A : \overline{K}]$. This r is also equal to the number of homomorphisms $\mathrm{Hom}_{\overline{K}}(A, \overline{K})$, which is also equal to the number of homomorphisms $\mathrm{Hom}_K(L, \overline{K})$. We can now formulate this result as a theorem.

Theorem 16. *Let L be a finite extension of K. (1) L is separable if and only if $L \otimes_K \overline{K}$ is reduced, and purely inseparable if and only if $L \otimes_K \overline{K}$ is local; (2) L is separable if and only if for all algebraic extensions Ω, we have $L \otimes_K \Omega$ reduced, and purely inseparable if and only if $L \otimes_K \Omega$ is local; (3) If L is separable, then $\varphi : L \otimes_K \overline{K} \to \overline{K}^n$ such that $\varphi(l \otimes_k) = (k\varphi_1(l), \ldots, k\varphi_n(l))$, where φ_i are distinct homomorphisms $L \to \overline{K}$, is an isomorphism.*

Proof. (1) We have seen that if L is separable, this is the same thing as saying that $A = L \otimes_K \overline{K}$ has $[L : K]$ factors $\overline{K}$. This is equivalent to saying that A is reduced, since the dimension of A over $\overline{K}$ is also equal to $[L : K]$. If L is purely inseparable, then there is only one homomorphism of L into $\overline{K}$, so A has only one homomorphism into $\overline{K}$; but this means that there is only one factor, which is to say that A is local.

(2) If Ω is an algebraic extension, then $L \otimes_K \Omega$ embeds into $L \otimes_K \overline{\Omega} = L \otimes_K \overline{K}K$ as a subring. One

can easily check that a subring of a reduced algebra is reduced, and similarly a subring of a local algebra is local.

(3) Exercise. ■

Remark 10. In general, for modules M, N, P over a ring R, it is *not* true that if $M \hookrightarrow N$ then $M \otimes_R P \hookrightarrow N \otimes_R P$. If R is a field, i.e. all our modules are vector spaces, then this becomes true.

5.3 Primitive element theorem.

Theorem 17. *Let L be a finite separable extension of K. Then it has only finitely many sub-extensions $K \subset E \subset L$.*

Proof. Let E be sub-extension. Perform a base-change to $E \otimes_K \overline{K} \hookrightarrow L \otimes_K \overline{K}$; this is a (reduced) $\overline{K}$-subalgebra. Moreover, $E \otimes_K \overline{K} \simeq \overline{K}^m$ and $L \otimes_K \overline{K} \simeq \overline{K}^n$. We know that $\overline{K}$ is generated by **idempotents** (x such that $x^2 = x$), namely, these are just $(0, 0, \ldots, 1, 0, \ldots, 0)$ with the 1 in the ith place for $i = 1, \ldots, m$. On the other hand, $L \otimes_K \overline{K} \simeq \overline{K}$ has only finitely many idempotents: $(a_1, \ldots, a_i, \ldots, a_n)$ is idempotent if and only if all a_i are either 0 or 1. Hence, there are only finitely many ways of generating subalgebras this way. ■

Now we state the "Primitive element theorem" as a corollary.

Corollary 9. Let L be a finite separable extension. Then there exists $\alpha \in L$ such that $L = K(\alpha)$.

Proof. If L, K are infinite, then L cannot be a finite union of proper sub-extensions (a vector space over an infinite field is not a finite union of subspaces). If L, K are finite, we have described all finite extensions, and have seen that they are generated by one element. ■

We now look at two examples.

Example 20. (1) Take $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, all subextensions are quadratic, and no quadratic polynomial has $\sqrt{2} + \sqrt{3}$ for a root, it must be a primitive element.

(2) (Counter-example) Let $K = \mathbb{F}_p$ and consider $K(X, Y)$ as an extension of $K(X^p, Y^p)$. This has degree p^2. Now any $\alpha \in K(X, Y)\ K(X^p, Y^p)$ is purely inseparable of degree p over $K(X^p, Y^p)$, since $\alpha^p \in K(X^p, Y^p)$, so no element like this can generate our extension.

5.4 Normal extensions.

Definition 20. A **normal extension** of K is a splitting field of a family of polynomials in $K[x]$.

For instance, a splitting field of a single polynomial is normal.

Theorem 18. *The following conditions are equivalent for an extension L of K: (1) For any $x \in L$, the minimal polynomial $P_{\min}(x, K)$ splits in L;*

(2) L is normal;

(3) All homomorphisms from L to $\overline{K}$ have the same image;

(4) $\mathrm{Aut}(L/K)$ acts transitively on $\mathrm{Hom}_K(L, \overline{K})$.

Proof. (1) $\Rightarrow$ (2): Take $(P_i)_{i\in I} = \{P_{\min}(x, K) | x \in L\}$. Then L is a splitting field of this family.

(2) $\Rightarrow$ (3): Let S be the set of roots of $P_i, i \in I$ in L, and S' the set of roots of $P_i, i \in I$ in $\overline{K}$. Any $\varphi : L \to \overline{K}$ sends S to S', but S generates L over K, so $\varphi(S)$ determines $\varphi(L)$.

(3) $\Rightarrow$ (4): If $j, j' \in \mathrm{Hom}_K(L, \overline{K})$ then they are isomorphisms from L to its image L'. Hence we can produce $j^{-1} \circ j' : L(\to L') \to L$, that is, $j^{-1} \circ j' \in \mathrm{Aut}(L/K)$ and it sends j to j'.

(4) $\Rightarrow$ (1): Consider $P_{\min}(x, K)$ with roots $\alpha_1, \ldots, \alpha_n \in \overline{K}$. A map $K(x) \to K(\alpha_i)$ extends to $j_i : L \to \overline{K}, x \mapsto \alpha_i$ by the theorem on extensions of homomorphisms. Now there exist $\theta_i \in \mathrm{Aut}(()L/K)$ such that $j_1\theta_i = j_i \to \alpha_i \in j_1(L)$, hence all roots are in $j_1(L)$ and the polynomial splits over $j_1(L)$. But this means that the polynomial also splits over L. ■

5.5 Galois extensions.

We are now ready to give the main definition of this course.

Definition 21. A **Galois extension** is a normal and separable extension.

This will be the central object of Galois theory.

Theorem 19. *Let L be a finite extension of K. Then the number of automorphisms of L over K is less than or equal to $[L : K]$, with equality if and only if L is Galois.*

Proof. We know that $\mathrm{Aut}(L/K)$ acts freely on $\mathrm{Hom}_K(L, \overline{K})$. So the number of automorphisms is equal to the cardinality of an orbit of this action, which is less than or equal to the cardinality of the set itself. We have equality if and only if the action is transitive, and we have just seen

in the previous theorem that this means that L is normal over K. Then the size of $\mathrm{Aut}(L/K)$ is less than or equal to the size of $\mathrm{Hom}_K(L, \overline{K})$ (equality iff normal), which is less than or equal to $[L : K]$ (equality iff separable). Therefore the size of $\mathrm{Aut}(L/K)$ is less than or equal to $[L : K]$, with equality iff Galois. ■

Remark 11. Some remarks on normal extensions. Let L/K be normal.

(1) Let $\varphi : L_1 \xrightarrow{\sim} L_2$ be an isomorphism of subextensions. Then φ extends to an automorphism of L. To see this, we embed $L \hookrightarrow \overline{K}$ and remark that φ extends to a map into $\overline{K}$ but all such extended maps have the same image, namely L.

(2) The group $\mathrm{Aut}(L/K)$ acts transitively on the roots of any irreducible polynomial in $K[x]$. Again, an isomorphism of stem fields extends to an isomorphism of L.

(3) If $\mathrm{Aut}(L/K)$ fixes $x \notin K$ then x is purely inseparable over K. This is clear because if so, $P_{\min}(x, K)$ must have x as the only root. In particular, if L is Galois, then $L^{\mathrm{Aut}(L/K)} = K$. (Notation: If G is a group acting on a set X, then $X^G = \{x \in X : gx = x \forall g \in G\}$ is the set of invariants.

Definition 22. If L is Galois, the **Galois group** $G = \mathrm{Gal}(L/K)$ is just $\mathrm{Aut}(L/K)$. (Then $L^{\mathrm{Gal}(()L/K)} = K$.)

5.6 Artin's theorem.

So, motivated by this remark—that the field of invariants of L under the action of G is K—we formulate and prove an important theorem.

Theorem 20 (Artin)**.** *Let L be a field, and $G \subset \mathrm{Aut}(L)$.*

(1) If G acts with finite orbits (i.e., all orbits of G are finite), then L is a Galois extension of L^G;

(2) If $|G| = n$ then $[L : L^G] = n$, and G is the Galois group.

Remark 12. Notice that finite orbits and finiteness are *not the same thing*! It's typical for Galois groups to act with finite orbits: if $G = \mathrm{Gal}(L/K)$ and $x \in L$ is a root of a polynomial of some finite degree, its splitting field is finite over K, so the orbit of x is also finite. (It consists of roots of $P_{\min}(x, K)$.) But $\mathrm{Gal}(L/K)$ can be infinite when L is not finite over K: for instance, if $K = \mathbb{F}_p$ and $L = \overline{\mathbb{F}}_p$.

Proof of Artin's theorem. (1) Take $x = x_1 \in L$ L^G and let $x_1, x_2, \ldots, x_k$ be the orbit of x. Now $P(x) = \prod_{i=1}^{k}(x - x_i)$ is G-invariant! Then $P \in L^G[x]$, P is separable (all x_i are distinct), and L is

a splitting field of P. Therefore L is Galois over L^G.

(2) Suppose that $|G| = n$. Then the size of any orbit is less than or equal to n. Take x as above: then $[L^G(x) : L^G] \leq n$. We claim that this implies $[L : L^G] \leq n$. If we already knew that L was finite over L^G, this would be very easy: in fact, a direct consequence of the primitive element theorem. We don't know yet, though, that L is finite. Indeed, take x such that $[L^G(x) : L^G]$ is maximal, and take $y \in L$. Then $L^G(x, y)$ is finite over L, and we can apply the primitive element theorem: $L^G(x, y) = L^G(z)$. But $[L^G(x) : L^G] \geq [L^G(z) : L^G]$, hence $L^G(x) = L^G(z)$, so $y \in L^G(x)$. Since we can do this for any y, we can conclude that $L = L^G(x)$. In particular, $[L : L^G] \leq n$. Now, if $[L : L^G] < n$, then L cannot have n automorphisms over L^G, but $G \subset \mathrm{Aut}(L/L^G)$, a contradiction. Therefore we conclude that $[L : L^G] = n$, and $G = \mathrm{Aut}(L/L^G)$. ■

5.7 Week 5 Quiz

⋆ 1. Fix a field k and a finite k-algebra A. Which of the following are true?

A finite k-algebra A is reduced (has no nilpotent elements) if and only if it is a field. This is *false*; for example,

Let $A \simeq A/\mathfrak{m}_1^{n_1} \times \cdots \times A/\mathfrak{m}_r^{n_r}$, where $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are the maximal ideals in A. Let A_{red} be the reduction of A, that is, the quotient of A by te ideal of nilpotent elements. Then $A_{\text{red}} \simeq A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_r$. This is *true*; by

Let L/k be a finite field extension of degree d. Then the number of k-homomorphisms $L \to \bar{k}$ is d. This is *false* in general, only true when L is separable;

Let L/k be a finite field extension of degree d. Then the number of k-homomorphisms $L \to \bar{k}$ is r, where r is the number of maximal ideals in $A = L \otimes_k \bar{k}$. This is *true*;

Let L/k be a finite field extension. It is separable if and only if $L \otimes_k \bar{k}$ is a reduced $\bar{k}$-algebra. This is *true*;

⋆ 2. Recall that if L/k is a finite separable field extension, then $L = k(\alpha)$ for some $\alpha \in L$. For which fields does equality hold?

$\mathbb{Q}(\sqrt{2}, e^{2\pi\imath/3}) = \mathbb{Q}(\sqrt{2} + e^{2\pi\imath/3})$**.** This is *true*; we know that since $\mathbb{Q}$ has characteristic 0 any extension is separable, so the primitive element theorem must hold in this case. More specifically, let $\gamma = \sqrt{2} + e^{2\pi\imath/3}$. Then:

$$\begin{aligned}
\gamma^1 &= \sqrt{2} + e^{2\pi\imath/3} \\
\gamma^2 &= 1 + (-1 + 2\sqrt{2})e^{2\pi\imath/3} \\
\gamma^3 &= (1 - \sqrt{2}) + (6 - 3\sqrt{2})e^{2\pi\imath/3} \\
\gamma^4 &= -8 + 4\sqrt{2} + (-11 + 8\sqrt{2})e^{2\pi\imath/3} \\
\gamma^4 - 4\gamma^2 + 12 &= -8 + 4\sqrt{2} + (-11 + 8\sqrt{2})e^{2\pi\imath/3} - 4 + (4 - 8\sqrt{2})e^{2\pi\imath/3} + 12 \\
&= 4\sqrt{2} - 7e^{2\pi\imath/3}
\end{aligned}$$

And we see that from here, we can obtain $-(\gamma^4 - 4\gamma^2 - 4\gamma + 12)/11 = e^{2\pi\imath/3}$ and $(\gamma^4 - 4\gamma^2 + 7\gamma + 12)/16 = \sqrt{2}$. Therefore indeed $\mathbb{Q}(\sqrt{2}, e^{2\pi\imath/3}) = \mathbb{Q}(\sqrt{2} + e^{2\pi\imath/3})$.

$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\imath/3}) = \mathbb{Q}(\sqrt[3]{2} \cdot e^{2\pi\imath/3})$**.** This is *false*; writing $\sqrt[3]{2} \cdot e^{2\pi\imath/3} = 2^{1/3} \cdot (-1)^{2/3} = \eta$, we see:

$$\begin{aligned}\eta^1 &= 2^{1/3} \cdot (-1)^{2/3} \\ \eta^2 &= -2^{2/3} \cdot (-1)^{1/3} \\ \eta^3 &= 2\end{aligned}$$

Hence $[\mathbb{Q}(\sqrt[3]{2} \cdot e^{2\pi\imath/3} : \mathbb{Q}] = 3$, and yet $\left\{1, 2^{1/3}, 2^{2/3}, e^{2\pi\imath/3}, e^{4\pi\imath/3}\right\}$ is a basis of $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\imath/3})$, making $[\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\imath/3}) : \mathbb{Q}] = 5$.

$\mathbb{F}_{2^3} = \mathbb{F}_2(\zeta)$**, where** ζ **is a primitive third root of unity.** This is *false*; we know $\mathbb{F}_{2^3} \simeq \mathbb{F}_2[x]/(x^3 + x^2 + x + 1)$ and $x^3 + x^2 + x + 1 = (x^4 - 1)/(x - 1)$, but this doesn't have ζ as a root. Therefore $\zeta \notin \mathbb{F}_{2^3}$, so $\mathbb{F}_{2^3} \neq \mathbb{F}_2(\zeta)$.

$\mathbb{F}_{2^2} = \mathbb{F}_2(\zeta)$**, where** ζ **is a primitive third root of unity** This is *true*; we know that $\mathbb{F}_{2^2} \simeq \mathbb{F}_2[x]/(x^2 + x + 1)$, and $x^2 + x + 1 = (x^3 - 1)/(x - 1)$ is the third cyclotomic polynomial so it has ζ as a root. Therefore $\mathbb{F}_{2^2} = \mathbb{F}_2(\zeta)$.

⋆ 3. Which of the following statements are true?

$\mathbb{F}_{p^n}/\mathbb{F}_p$ **is a Galois extension.** This is *true*;

$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\imath/3})/\mathbb{Q}$ **is a normal extension.** This is *true*;

$k(x)/k$**, where** x **is an indeterminate, is a Galois extension of** k**.** This is *false*;

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ **is a normal extension.** This is *false*; $\mathbb{Q}(\sqrt[3]{2})$ is a stem field for the polynomial $x^3 - 2$, but is not a splitting field. In particular the complex third roots of unity (say, ζ, ζ^2) are not in this field, yet $\zeta \cdot \sqrt[3]{2}$ is a root of the polynomial.

⋆ 4. Which of the following statements are true?

Every finite extension of $\mathbb{F}_p$ **is Galois.** This is *true*;

$|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n!$ This is *xxx*; the polynomial $x^{p^n} - x$ has p^n distinct roots, each of order p^n, so

If L/k is a finite extension, then $|\mathrm{Aut}(L/k)| \leq [L:k]$, with equality if an only if L/k is Galois.

$|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$. This is *true*; the set of automorphisms must permute the roots of $x^3 - 2$, but only one such root is an element of $\mathbb{Q}(\sqrt[3]{2})$.

$|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 3$. This is *false*.

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is Galois. This is *false*.

$\rightarrow$ 5. Which of the following statements are true?

Let $F \subset \mathbb{C}$ be a subfield stable under complex conjugation. Then $F/F \cap \mathbb{R}$ is a Galois extension. This is *false*; consider $F = \mathbb{Q}(\sqrt[3]{2} \cdot e^{2\pi\imath/3})$. Then since $(e^{2\pi\imath/3})^2 = e^{4\pi\imath/3} = e^{-2\pi\imath/3} = \overline{(e^{2\pi\imath/3})}$, the field is stable under complex conjugation. Yet $F/F \cap \mathbb{R} = \mathbb{Q}(\sqrt[3]{2} \cdot e^{2\pi\imath/3})/\mathbb{Q}$ which is not a separable extension.

Let $F \subset \mathbb{C}$ be a subfield. Then $F/F \cap \mathbb{R}$ has degree 2. This is *false*; consider $F = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi\imath/3}) = \mathbb{Q}[x]/(x^3 - 2)$. Then $F \cap \mathbb{R} = \mathbb{Q}(\sqrt[3]{2})$ and hence $F/F \cap \mathbb{R} = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi\imath/3})/\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})(e^{2\pi\imath/3}$ which is a degree 3 extension.

An algebraic closure $\bar{Q}$ is Galois over $\mathbb{Q}$. This is *true*;

An algebraic closure $\bar{\mathbb{F}_p}$ is Galois over $\mathbb{Q}$. This is *true*;

An algebraic closure $\overline{\mathbb{F}_p(T)}$ is Galois over $\mathbb{F}_p(T)$. This is *false*;

$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acting on $\bar{\mathbb{Q}}$ has an infinite orbit. This is *true*;

5.8 Graded Assignment

Question 8. We consider the polynomial $P(X) = X^4 + X^3 + 1$. Is it true that P

a) is irreducible over $\mathbb{F}_2$? b) has a root in $\mathbb{F}_4$? c) is irreducible over F_4? d) is irreducible over F_8? e) has a root in F_16? f) has a root in F_32? g) has a root in F_64? h) is irreducible over F_64?

Solution. Consider the polynomial $P(X) = X^4 + X^3 + 1$. Is it true that P

a) is irreducible over $\mathbb{F}_2$? Yes; we merely check $P(0) = 0 + 0 + 1 = 1$ and $P(1) = 1 + 1 + 1 = 1$, confirming that P has no roots in $\mathbb{F}_2$, and therefore no linear factors. Now we consider quadratic factors. The polynomials of degree 2 over $\mathbb{F}_2$ are $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$.

Yes. Otherwise it either has a root or is the product of two (possibly equal) irreducible polynomials of degree 2. But there is only one such polynomial over a field of 2 elements, namely $X^2 + X + 1$, and P is not its square.

b) has a root in $\mathbb{F}_4$? $4 = 2^2$ so we need a monic irreducible quadratic over F_2; our options are $x^2 + 1 = (x + 1)^2$, $x^2 + x = x(x + 1)$, and $x^2 + x + 1$, which is irreducible over F_2. Let α be a root of this polynomial, so $\alpha^2 = \alpha + 1$. Then we have

$$\begin{aligned}\alpha^1 &= \alpha \\ \alpha^2 &= \alpha + 1 \\ \alpha^3 &= \alpha^2 + \alpha \\ &= \alpha + 1 + \alpha \\ &= 1\end{aligned}$$

Now we try to find roots. (We already know there are no roots in $\mathbb{F}_2 \subset \mathbb{F}_4$.)

$$\begin{aligned}P(\alpha) &= \alpha^4 + \alpha^3 + 1 = \alpha + 1 + 1 = \alpha \\ P(\alpha + 1) &= (\alpha + 1)^4 + (\alpha + 1)^3 + 1 = \alpha^4 + 1 + \alpha^3 + 1 + 1 = \alpha + 1 + 1 + 1 + 1 = \alpha\end{aligned}$$

Therefore there are no roots in $\mathbb{F}_4$.

No. Since the polynomial is irreducible over $\mathbb{F}_2$, its root generates a degree four extension of $\mathbb{F}_2$, and $\mathbb{F}_4$ is only a degree-two extension of $\mathbb{F}_2$.

c) is irreducible over $\mathbb{F}_4$? Consider the following table of elements of $\mathbb{F}_4$.

Bit string	n	α^n	Polynomial in α
00	·	·	0
10	1	α^1	α
11	2	α^2	$\alpha + 1$
01	3	α^3	1

We know that there are no factors with coefficients all in $\mathbb{F}_2 \subset \mathbb{F}_4$, so we need only check .

Map $\alpha \mapsto \eta^{10} = \eta^3 + \eta$ (so $\alpha + 1 = \alpha^2 \mapsto \eta^{20} = \eta^5 = \eta^3 + \eta + 1$.

$x^4 + x^3 + 1 = (x + \eta)(x + \eta^2)(x + \eta^4)(x - \eta^8)$

$$(x + \eta)(x + \eta^2) = x^2 + (\eta^2 + \eta)x + \eta^3 = x^2 + \eta^{13}x + 1$$

$$(x + \eta)(x + \eta^4) = x^2 + (\eta + \eta^4)x + \eta^5 = x^2 + \eta^5 x + \eta^5$$

Which pulls back to $x^2 + \alpha x + \alpha$.

$$(x + \eta)(x + \eta^8) = x^2 + (\eta + \eta^8)x + \eta^9 = x^2 + \eta^{14}x + \eta^9$$

$$(x + \eta^2)(x + \eta^8) = x^2 + (\eta^2 + \eta^8)x + \eta^{10} = x^2 + \eta^{10}x + \eta^{10}$$

Which pulls back to $x^2 + \alpha^2 x + \alpha^2$.

$$\begin{aligned}(x^2 + \alpha x + \alpha)(x^2 + \alpha^2 x + \alpha^2) &= x^4 + \alpha^2 x^3 + \alpha^2 x^2 + \alpha x^3 + \alpha^3 x^2 + alpha^3 x + \alpha x^2 + \alpha^3 x + \alpha^3 \\ &= x^4 + (\alpha^2 + \alpha)x^3 + (\alpha^2 + \alpha^3 + \alpha)x^2 + (\alpha^3 + \alpha^3)x + (\alpha^3)1 \\ &= x^4 + x^3 + 1\end{aligned}$$

$x^2 + \alpha^2$ $x^2 + x + \alpha$ $x^2 + x + \alpha^2$ $x^2 + \alpha x + 1$ $x^2 + \alpha^2 x + 1$ $x^2 + \alpha x + \alpha$ $x^2 + \alpha x + \alpha^2$ $x^2 + \alpha^2 x + \alpha$ $x^2 + \alpha^2 x + \alpha^2$

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + (bd)1$$

No. If it were irreducible over $\mathbb{F}_4$ it would not have a root in $\mathbb{F}_{16}$ and $\mathbb{F}_{16}$ is it splitting field as we have seen in the lectures.

d) is irreducible over $\mathbb{F}_8$?

Bit string	n	β^n	Polynomial in β
000	.	.	0
010	1	β^1	β
100	2	β^2	β^2
011	3	β^3	$\beta + 1$
110	4	β^4	$\beta^2 + \beta$
111	5	β^5	$\beta^2 + \beta + 1$
101	6	β^6	$\beta^2 + 1$
001	7	β^7	1

$$
\begin{aligned}
P(\beta) &= \beta^4 + \beta^3 + 1 \\
&= \beta^2 + \beta + \beta + 1 + 1 \\
&= \beta^2 \\
P(\beta^2) &= \beta^8 + \beta^6 + 1 \\
&= \beta + \beta^2 + 1 + 1 \\
&= \beta^2 + \beta \\
P(\beta^3) &= \beta^{12} + \beta^9 + 1 \qquad\qquad = \beta^5 + \beta^2 + 1 \\
&= \beta^2 + \beta + 1 + \beta^2 + 1 \\
&= \beta \\
P(\beta^4) &= \beta^{16} + \beta^{12} + 1 \\
&= \beta^2 + \beta^5 + 1 \\
&= \beta^2 + \beta^2 + \beta + 1 + 1 \\
&= \beta \\
P(\beta^5) &= \beta^{20} + \beta^{15} + 1 \\
&= \beta^6 + \beta + 1 \\
&= \beta^2 + 1 + \beta + 1 \\
&= \beta \\
P(\beta^6) &= \beta^{24} + \beta^{18} + 1 \\
&= \beta^3 + \beta^4 + 1 \\
&= \beta + 1 + \beta^2 + \beta + 1 \\
&= \beta^2
\end{aligned}
$$

Bit string	n	η^n	Polynomial in η
0000	.	.	0
0001	0	η^0	1
0010	1	η^1	η
0100	2	η^2	η^2
1000	3	η^3	η^3
1001	4	η^4	η^3+1
1011	5	η^5	$\eta^3+\eta+1$
1111	6	η^6	$\eta^3+\eta^2+\eta+1$
0111	7	η^7	$\eta^2+\eta+1$
1110	8	η^8	$\eta^3+\eta^2+\eta$
0101	9	η^9	η^2+1
1010	10	η^{10}	$\eta^3+\eta$
1101	11	η^{11}	$\eta^3+\eta^2+1$
0011	12	η^{12}	$\eta+1$
0110	13	η^{13}	$\eta^2+\eta$
1100	14	η^{14}	$\eta^3+\eta^2$

Yes. $\mathbb{F}_8$ is a degree 3 extension of $\mathbb{F}_2$ and $\gcd(3,4)=1$; we have seen in the lectures that in this situation the polynomial remains irreducible.

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$

e) has a root in $\mathbb{F}_{16}$? Yes. Since $\deg P = 4$ and P is irreducible in $\mathbb{F}_2[X]$, by Prop. # we have that $\mathbb{F}_{2^4} = \mathbb{F}_{16}$ is a splitting field for P, that is, we can write $F_{16} = F_2[x]/(x^4+x^3+1)$. Let η be a root of x^4+x^3+1. Then we can write the elements of $\mathbb{F}_16$ as:

Yes, $\mathbb{F}_{16}$ is it splitting field as we have seen in the lectures.

f) has a root in $\mathbb{F}_{32}$? $32 = 2^5$. We can represent $\mathbb{F}_{32}$ as $\mathbb{F}_2[x]/(x^5+x^2+1)$.

No. It is even irreducible over $\mathbb{F}_{32}$ by the same reason as in (d): $\gcd(5,4)=1$.

g) has a root in $\mathbb{F}_{64}$? We can represent $\mathbb{F}_{64} = \mathbb{F}_{2^6}$ as $\mathbb{F}_2[x]/(x^6+x+1)$.

$64 = 2^6$, and $2|6$ and $3|6$, so $\mathbb{F}_4 \subset \mathbb{F}_{64}$ and $\mathbb{F}_8 \subset \mathbb{F}_{64}$, with $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$ since $2 \not| 3$ (and therefore $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_8$.

No. Otherwise, $\mathbb{F}_{64}$ would contain $\mathbb{F}_{16}$ and it does not, since $4 \not| 6$.

h) is irreducible over $\mathbb{F}_{64}$? Since $\mathbb{F}_4 \subset \mathbb{F}_{64}$ we should be able to factor x^4+x^3-1 into $x^2+\sigma(\alpha)x+$

Bit string	n	μ^n	Polynomial in μ
00000	.	.	0
00001	0	μ^0	1
00010	1	μ^1	μ
00100	2	μ^2	μ^2
01000	3	μ^3	μ^3
10000	4	μ^4	μ^4
00101	5	μ^5	$\mu^2 + 1$
01010	6	μ^6	$\mu^3 + \mu$
10100	7	μ^7	$\mu^4 + \mu^2$
01101	8	μ^8	$\mu^3 + \mu^2 + 1$
11010	9	μ^9	$\mu^4 + \mu^3 + \mu$
10001	10	μ^{10}	$\mu^4 + 1$
00111	11	μ^{11}	$\mu^2 + \mu + 1$
01110	12	μ^{12}	$\mu^3 + \mu^2 + \mu$
11100	13	μ^{13}	$\mu^4 + \mu^3 + \mu^2$
11101	14	μ^{14}	$\mu^4 + \mu^3 + \mu^2 + 1$
11111	15	μ^{15}	$\mu^4 + \mu^3 + \mu^2 + \mu + 1$

$\sigma(\alpha))(x^2+\sigma(\alpha^2)x+\sigma(\alpha^2)$ by a suitable homomorphism $\sigma:\mathbb{F}_4\to\mathbb{F}_{64}$. Now we know that if γ is a root of x^6+x+1 so that $\gamma^6=\gamma+1$, then γ has order $63=3^2\cdot 7$, so that suggests (since we need $\sigma(\alpha)$ to have order 3) that $\sigma(\alpha)=\gamma^{21}$ or $\sigma(\alpha)=\gamma^{42}$, as $(\gamma^{21})^3=\gamma^{63}=1$ and $(\gamma^{42})^3=\gamma^{126}=(\gamma^{63})^2=1$ but $(\gamma^{42})^2=\gamma^{84}=\gamma^{21}$.

Bit string	n	γ^n	Polynomial in γ
000000	.	.	0
000010	1	γ^1	γ^1
000100	2	γ^2	γ^2
001000	3	γ^3	γ^3
010000	4	γ^4	γ^4
100000	5	γ^5	γ^5
000011	6	γ^6	$\gamma+1$
000110	7	γ^7	$\gamma^2+\gamma$
001100	8	γ^8	$\gamma^3+\gamma^2$
011000	9	γ^9	$\gamma^4+\gamma^3$
110000	10	γ^{10}	$\gamma^5+\gamma^4$
100011	11	γ^{11}	$\gamma+1+\gamma^5$
000101	12	γ^{12}	γ^2+1
001010	13	γ^{13}	$\gamma^3+\gamma$
010100	14	γ^{14}	$\gamma^4+\gamma^2$
101000	15	γ^{15}	$\gamma^5+\gamma^3$
010011	16	γ^{16}	$\gamma^4+\gamma+1$
100110	17	γ^{17}	$\gamma^5+\gamma^2+\gamma$
001111	18	γ^{18}	$\gamma^3+\gamma^2+\gamma+1$
011110	19	γ^{19}	$\gamma^4+\gamma^3+\gamma^2+\gamma$
111100	20	γ^{20}	$\gamma^5+\gamma^4+\gamma^3+\gamma^2$
111011	21	γ^{21}	$\gamma^5+\gamma^4+\gamma^3+\gamma+1$
⋮	⋮	⋮	⋮
111010	42	γ^{42}	$\gamma^5+\gamma^4+\gamma^3+\gamma$
⋮	⋮	⋮	⋮

So we set $\sigma(\alpha)=\gamma^{42}$ (and hence $\sigma(\alpha+1)=\gamma^{21}=\gamma^{42}+1$:

$$x^4+x^3-1=(x^2+\gamma^{42}x+\gamma^{42})(x^2+\gamma^{21}x+\gamma^{21})$$

No. $\mathbb{F}_{64}$ contains $\mathbb{F}_4$ since $2|6$ and our polynomial is the product of two quadratic factors over $\mathbb{F}_4$. ■

Question 9. a) Let p be a prime number. Prove that the polynomial $X^{p-1}+X_{p-2}+\cdots+X+1 = \frac{X^p-1}{X-1}$ is irreducible over $\mathbb{Q}$ (a possible hint: one can try ot use Eisenstein criterion after a suitable variable change).

Proof. Let $X = y+1$, so we now have

$$\begin{aligned}\frac{(y+1)^p-1}{y+1-1} &= \frac{y^p + \binom{p}{2}y^{p-1} + \cdots + \binom{p}{p-1}y + 1 - 1}{y} \\ &= y^{p-1} + \binom{p}{2}y^{p-2} + \cdots + p\end{aligned}$$

Now p divides all the binomial coefficients, but since the last coefficient is exactly equal to p, clearly p^2 doesn't divide it. Therefore by Eisenstein we have that the polynomial in y is irreducible. Moreover, if the original polynomial in X was reducible, we would have it equal to $Q(X)R(X)$, but then $Q(y+1)R(y+1)$ would be a factorization of the polynomial in y. Hence the original polynomial in X is irreducible. ■

Question 10. b) Set $\zeta = e^{2\imath\pi/7}$ and $L = \mathbb{Q}(\zeta)$. Let $M = L \cap \mathbb{R}$. Find the minimal polynomial of ζ over $\mathbb{Q}$ and the degree of L over $\mathbb{Q}$.

Solution. We see that $\zeta^7 = e^{2\imath\pi} = 1$, so it is a root of $x^7 - 1 = (x-1)(x^6+x^5+x^4+x^3+x^2+1)$. Now $x^6+x^5+x^4+x^3+x^2+x+1$ is irreducible from what we showed in part (a), and $[L:\mathbb{Q}] = 6$ since $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ is a basis for $L = \mathbb{Q}(\zeta)$. Thus we have the minimal polynomial for ζ.

By part (a), the polynomial $x^6+x^5+x^4+x^3+x^2+x+1$ is irreducible and has $\zeta = e^{2\pi\imath/7}$ as a root, so it must be the minimal polynomial of ζ. The extension $L = \mathbb{Q}(\zeta)$ must have degree 6 over $\mathbb{Q}$. ■

Question 11. c) Find the minimal polynomial of ζ over M (hint: what is $\zeta + 1/\zeta$?) and the degrees $[L:M]$ and $[M:\mathbb{Q}]$.

Solution. We note that

$$\zeta + 1/\zeta = e^{2\imath\pi/7} + e^{-2\imath\pi/7} = \cos 2\pi/7 + \imath \sin 2\pi/7 + \cos -2\pi/7 + \imath \sin -2\pi/7 = 2\cos 2\pi/7$$

Note also that $\zeta^{-1} = \zeta^6$ since $\zeta \cdot \zeta^6 = \zeta^7 = 1$. Hence

$$\begin{aligned}
(\zeta + \zeta^6)^3 &= \zeta^3 + 3\zeta^2 \cdot \zeta^6 + 3\zeta \cdot (\zeta^6)^2 + (\zeta^6)^3 \\
&= \zeta^3 + 3\zeta^8 + 3\zeta^{13} + \zeta^{18} \\
&= \zeta^3 + 3\zeta + 3\zeta^6 + \zeta^4 \\
(\zeta + \zeta^6)^2 &= \zeta^2 + 2\zeta \cdot \zeta^6 + (\zeta^6)^2 \\
&= \zeta^2 + 2\zeta^7 + \zeta^{12} \\
&= \zeta^2 + 2 + \zeta^5 \\
(\zeta + \zeta^6)^3 + \cdot(\zeta + \zeta^6)^2 - 2 \cdot (\zeta + \zeta^6) &= \zeta^3 + 3\zeta + 3\zeta^6 + \zeta^4 + \zeta^2 + 2 + \zeta^5 - 2\zeta - 2\zeta^6 \\
&= \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 + 1 \qquad = 1
\end{aligned}$$

So $\zeta + \zeta^{-1}$ is a root of $x^3 + x^2 - 2x - 1$, which is irreducible in $\mathbb{Q}$ (by, e.g., considering the polynomial modulo 2).

Since this polynomial has degree 3, we conclude that $[M : \mathbb{Q}] = 3$, whence $[L : M] = 2$ since $[L : \mathbb{Q}] = [L : M][M : \mathbb{Q}] = 6$.

Note $\zeta + 1/\zeta = 2\cos(2\pi/7) \in M = L \cap \mathbb{R}$. Thus the quadratic polynomial $(x - \zeta)(x - 1/\zeta) = x^2 - 2\cos(2\pi/7)x + 1$ has coefficients in M, and is irreducible over M, since $M \subset \mathbb{R}$ while the roots of this polynomial are non-real. Hence $x^2 - 2\cos(2\pi/7)x + 1$ is the minimal polynomial for ζ over M. It follows that $[L : M] = 2$, and so since $6 = [L : \mathbb{Q}] = [L : M][M : \mathbb{Q}] = 2[M : \mathbb{Q}]$, it also follows that $[M : \mathbb{Q}] = 3$. ■

Question 12. d) Let f be an automorphism of L over $\mathbb{Q}$. List all possibilities for $f(\zeta)$, then for $f(\cos(2\pi/7))$.

Solution. We see that $\zeta, \zeta^2, \ldots, \zeta^6$ all have order 7, so we can have $f_n(\zeta) = \zeta^n$, $n = 1, \ldots, 6$, that is, six possibilities for $f(\zeta)$.

Now if $\zeta \mapsto \zeta^n$, then $\cos(2\pi/7) = (\zeta + \zeta^6)/2 \mapsto (\zeta^n + \zeta^{6n})/2$.

$n = 1 : (\zeta + \zeta^6)/2$

$n = 2 : (\zeta^2 + \zeta^{12})/2 = (\zeta^2 + \zeta^5)/2$

$n = 3 : (\zeta^3 + \zeta^{18})/2 = (\zeta^3 + \zeta^4)/2$

$n = 4 : (\zeta^4 + \zeta^{24})/2 = (\zeta^4 + \zeta^3)/2$ (same as $n = 3$)

$n = 5 : (\zeta^5 + \zeta^{30})/2 = (\zeta^5 + \zeta^2)/2$ (same as $n = 2$)

$n = 6 : (\zeta^6 + \zeta^{36})/2 = (\zeta^6 + \zeta)/2$ (same as $n = 1$).

So there are only three possible images of $\cos(2\pi/7)$. ■

Question 13. Which of the following algebras are fields? Products of fields? Describe these fields.

Solution. a) $\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ We know that $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2-2)$, so $\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}(\sqrt[3]{2})[x]/(x^2-2)$. Now since x^2-2 is also irreducible over $\mathbb{Q}(\sqrt[3]{2})$, this is a field, with elements of the form $a + b \cdot \sqrt{2}$ where $a, b \in \mathbb{Q}(\sqrt[3]{2}$.

b) $\mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ This is isomorphic to $\mathbb{Q}(\sqrt[4]{2})[x]/(x^2-2)$, but x^2-2 is reducible over $\mathbb{Q}(\sqrt[4]{2}$ since $(\sqrt[4]{2})^2 = \sqrt{2}$. Hence this is not a field.

c) $\mathbb{F}_2(\sqrt{T}) \otimes_{\mathbb{F}_2(T)} \mathbb{F}_2(\sqrt{T})$ $F_2(\sqrt{T}) \simeq \mathbb{F}_2(T)[x]/(x^2-T)$, but $x^2 - T = (x - \sqrt{T})^2$ over $F_2(T)$. Hence the tensor product is not a field.

d) $\mathbb{F}_4(\sqrt[3]{T}) \otimes_{\mathbb{F}_4(T)} \mathbb{F}_4(\sqrt[3]{T})$. $F_4(\sqrt[3]{T}) \simeq \mathbb{F}_4(T)[x]/(x^3-T)$, and $x^3 - T$ is irreducible over $F_4(T)$.

$(x - \sqrt[3]{T})(x^2 + a \cdot x + (\sqrt[3]{T})^2) = x^3 + ax^2 + (\sqrt[3]{T})^2 x + \sqrt[3]{T}x^2 + a\sqrt[3]{T}x + T) = x^3 + (a + \sqrt[3]{T})x^2 + (a + \sqrt[3]{2} + (\sqrt[3]{2})^2)x + T$

$a + \surd$ ■

5.9 Week 6 Quiz

1. Which of the following statements are true?

Every quadratic extension F/k has automorphism group of order 2.

Every quadratic extension F/k of a field of characteristic zero is Galois.

Every quadratic extension F/k of a field of characteristic $p \neq 2$ is Galois.

$\mathbb{F}_2(X)/\mathbb{F}_2(X^2)$ **is a Galois extension.**

2. Which of the following statements are true?

Let F be the splitting field of $x^3 - 2$ over $\mathbb{Q}(\sqrt{-3})$ then $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{-3}) \simeq \mathbb{Z}/3\mathbb{Z}$.

Every cubic extension of $\mathbb{Q}$ is Galois.

$\mathrm{Aut}(()\mathbb{Q}(\sqrt[3]{2} \simeq \mathbb{Z}/3\mathbb{Z}$.

Let F be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Then $\mathrm{Gal}(F/\mathbb{Q}) \simeq S_3$.

3. Let $\Phi_d \in \mathbb{Q}[x]$ be the dth cyclotomic polynomial (the product of $x - \zeta^a$ for $\gcd(a, d) = 1$, where ζ is a primitive dth root of unity). Which of he following statements are true?

Φ_d has integral coefficients.

Φ_d is irreducible over $\mathbb{Q}$.

Φ_d is irreducible over $\mathbb{F}_p$ for every p.

$\Phi_8 = x^4 - 1$

$\Phi_8 = x^4 + 1$

$\Phi_{10} = x^4 - x^3 + x^2 - x + 1$

Part II

Exercises from Lang's "Algebra"