MH4920 — Galois Theory & Number Fields

Biweekly Quizzes

Jake Lai

Supervisor
Bernhard Schmidt

Study plan

Week	Topics	Readings
1	Algebraic foundations	LR 1
2	Field extensions; algebraic extensions; splitting fields & algebraic closure	DF 13.1, 2, 4
3	Separable extensions, normal extensions; cyclotomic extensions	DF 13.5, 6
4	Fundamental theorem of Galois theory; finite fields	DF 14.2, 3
5	Cyclotomic & abelian extensions; Galois groups of polynomials; insolvability of the quintic	DF 14.5, 6, 7
6	Historical motivation (Fermat's last theorem); number fields, number rings	M 1, 2
7	Number fields, number rings	M 2
8	Prime decomposition in number rings	M 3
9	Galois theory applied to prime decomposition	M 4
10	Ideal class group, unit group	M 5
11	Dirichlet's unit theorem; distribution of ideals in a number ring	M 6
12	Dedekind zeta function, class number formula	M 7
13	Statements of class field theory, reciprocity	M 8

LR = Lidl & Niederreiter, *Introduction to Finite Fields and their Applications*
DF = Dummit & Foote, *Abstract Algebra*
M = Marcus, *Number Fields*

Week 2 (24 Aug 2023)

Problem 1. Construct an algebraic extension F of $\mathbb{Q}$ such that there is no subfield K of F where $[K:\mathbb{Q}] = 2$.

Solution: Take any root α of x^3-2, which can be seen to be irreducible by either noting that x^3-2 is cubic and has no roots in $\mathbb{Q}$ (since $\sqrt[3]{2} \notin \mathbb{Q}$) or applying Eisenstein's criterion. Letting $F = \mathbb{Q}(\alpha)$, we see that $[F:\mathbb{Q}] = 3$; if $[K:\mathbb{Q}] = 2$, then $2 \mid 3$, a contradiction. (See also DF 13.2 Exercise 14.)

Problem 2. Let F be a field with $\mathrm{char}(F) = 7$. Find all roots of x^3-1 in F.

Solution: Note that $1^3-1=0$, so $x-1$ divides x^3-1 to produce x^2-x+1. Similarly, $3^2-3+1=7=0$ in F, so $x-3$ divides x^2-x+1 (say, via polynomial long division) to produce $x+2$. Thus, the roots are $1, 3, -2$; there are no more roots since $\deg(x^3-1) = 3$.

Problem 3. Let $f(x) = x^3+x^2+2x+2$. Find a zero divisor of $\mathbb{F}_3[x]/(f)$.

Solution: Note that $1^3+1^2+2(1)+2 = 6 = 0$ in $\mathbb{F}_3$, so $\theta - 1$ is a zero divisor of $\mathbb{F}_3[x]/(f)$ (following the notation of DF 13.1).

Alternatively, observe that

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

Grade obtained: 100%.

Week 4 (11 Sep 2023)

Problem 1. Prove that there are only finitely many roots of unity in any finite extension K of $\mathbb{Q}$.

Solution: Assume that $K/\mathbb{Q}$ contains infinitely many roots of unity, so that in particular it contains $\zeta_n = e^{2\pi i/n}$, where n is unbounded. Thus,

$$[K : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Since $\varphi(n)$ is unbounded, K is an infinite extension of $\mathbb{Q}$.

Problem 2. What is $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$?

Solution: Let $K = \mathbb{Q}(\zeta_n)$. Since K is the splitting field of $x^n - 1$ (or $\Phi_n(x)$) over $\mathbb{Q}$ which is separable, $K/\mathbb{Q}$ is Galois (and thus we can speak of the Galois group of $K/\mathbb{Q}$). For each $1 \leq a < n$ relatively prime to n, there exists an automorphism (say, σ_a) determined by the action $\zeta_n \mapsto \zeta_n^a$. Since $|G| = [K : \mathbb{Q}] = \varphi(n)$, G is exactly the group of all such σ_a.

Consider the map $f : (\mathbb{Z}/n\mathbb{Z})^\times \to G\ ;\ a \mapsto \sigma_a$. We have that

$$\sigma_a \sigma_b \zeta_n = \sigma_a \zeta_n^b = \zeta_n^{ab} = \sigma_{ab} \zeta_n,$$

so f is a group homomorphism. In particular, it is injective: suppose $\sigma_a = \sigma_b$, then $\zeta_n^a = \zeta_n^b$ so $a \equiv b \pmod n$. By $|G| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, f is bijective and hence an isomorphism. Therefore, $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Problem 3. Compute $[\mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4) : \mathbb{Q}]$.

Solution: Let $L = \mathbb{Q}(\zeta_7)$, $K = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4) \subseteq L$. As shown previously, $G = \mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma_2, \cdots, \sigma_6\}$. It suffices to determine the subgroup $H \leq G$ fixing the subfield K, i.e., fixing $\alpha := \zeta_7 + \zeta_7^2 + \zeta_7^4$.

$$\begin{aligned} 1\alpha &= \alpha & \sigma_4\alpha &= \sigma_2^2\alpha = \alpha \\ \sigma_2\alpha &= \sigma_2\zeta_7 + \sigma_2\zeta_7^2 + \sigma_2\zeta_7^4 & \sigma_5\alpha &= \sigma_3\sigma_4\alpha \neq \alpha \\ &= \zeta_7^2 + \zeta_7^4 + \zeta_7 = \alpha & & \\ \sigma_3\alpha &= \sigma_3\zeta_7 + \sigma_3\zeta_7^2 + \sigma_3\zeta_7^4 & \sigma_6\alpha &= \sigma_3\sigma_2\alpha \neq \alpha \\ &= \zeta_7^3 + \zeta_7^6 + \zeta_7^5 \neq \alpha & & \end{aligned}$$

Writing $\tau := \sigma_2$, we get that $H = \{1, \tau, \tau^2\}$ fixes K. Thus, $[K : \mathbb{Q}] = |G : H| = 6/3 = 2$.

$$\begin{array}{ccc} L & & 1 \\ \big|\,3 & & \big|\,3 \\ K & \longleftrightarrow & \{1, \tau, \tau^2\} \\ \big|\,2 & & \big|\,2 \\ \mathbb{Q} & & G \end{array}$$

Grade obtained: 80%.

Week 7 (28 Sep 2023)

It is given that $\Phi_{12}(x) = x^4 - x^2 + 1$.

Problem 1. Find the splitting fields of Φ_{12} over $\mathbb{F}_2$ and $\mathbb{F}_3$, and determine their Galois groups.

Solution: From Problem 2 below, the splitting fields of Φ_{12} over $\mathbb{F}_2$ and $\mathbb{F}_3$ are $\mathbb{F}_2[x]/(x^2 + x + 1) \cong \mathbb{F}_2[\zeta_3] \cong \mathbb{F}_4$ and $\mathbb{F}_3[x]/(x^2 + 1) \cong \mathbb{F}_3[i] \cong \mathbb{F}_9$ respectively. Since $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, the Galois groups of both splitting fields are the unique group of order 2. In particular, their nontrivial (Frobenius) automorphisms are $\zeta_3 \mapsto \zeta_3^2 = -\zeta_3$ and $i \mapsto i^3 = -i$ respectively.

Problem 2. Show that Φ_{12} is reducible in $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$.

Solution: In $\mathbb{F}_2[x]$, $\Phi_{12} = x^4 - x^2 + 1 = x^4 + x^2 + 1$. Since $(a+b)^2 = a^2 + b^2$, we have that $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. In $\mathbb{F}_3[x]$, $\Phi_{12} = x^4 - x^2 + 1 = x^4 + 2x^2 + 1 = (x^2 + 1)^2$. Since $\Phi_{12}(x) = 1$ for all values of x over both finite fields, Φ_{12} does not split further into linear factors.

Problem 3. Prove that $\Phi_{12} \mid (x^{p^2 - 1} - 1)$ for every prime $p \geq 5$. (Hint: $\Phi_{12} \mid (x^{12} - 1)$.)

Solution: Note that $p \equiv \pm 1$ or $\pm 5 \pmod{12}$. Thus, $p^2 - 1 \equiv 1^2 - 1$ or $5^2 - 1 \equiv 0 \pmod{12}$. Hence, $12 \mid (p^2 - 1)$, implying $x^{12} - 1$ divides $x^{p^2-1} - 1$. The statement follows immediately from the hint, obtained by noting that $\Phi_n \mid (x^n - 1)$ with $n = 12$.

Problem 4. Thus, prove that Φ_{12} is reducible in $\mathbb{F}_p[x]$ for all primes p.

Solution: We have proven the cases $p = 2, 3$. Let $p \geq 5$ be a prime. Since $x^{p^2-1} - 1$ splits completely over $\mathbb{F}_{p^2}$, so does Φ_{12}. Because $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, this implies that the minimal polynomial in $\mathbb{F}_p[x]$ for any element of $\mathbb{F}_{p^2}$ is at most degree 2. As such, Φ_{12} having all roots in $\mathbb{F}_{p^2}$ implies that it must have the (deg ≤ 2) minimal polynomial of one of those roots as a factor, hence is reducible (in particular, into the product of two quadratics uniquely).

Grade obtained: 75%.

Week 9 (23 Oct 2023)

Problem 1. Find a prime p such that (2) splits into exactly six prime ideals in $\mathbb{Z}[\zeta_p]$.

Solution: Since $\mathbb{Q}(\zeta_p)$ is a normal extension of $\mathbb{Q}$, all the ramification indices e_i and inertial degrees f_i of $Q_i \mid (2)$ are equal; so $ref = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Since clearly 2 does not divide p, it is unramified in $\mathbb{Q}(\zeta_p)$. Hence, we have $r = 6 \mid (p - 1)$, and need only check primes $p = 7, 13, 19, 31, \cdots$. We will use the fact that f is the multiplicative order of p mod n.

p	f	$(p-1)/f = r$
7	3	$6/3 = 2$
13	12	$12/12 = 1$
19	18	$18/18 = 1$
31	5	$30/5 = 6$

Therefore, (2) splits into exactly six primes in $\mathbb{Z}[\zeta_{31}]$.

Problem 2. Let $n \in \mathbb{Z}^+$, $q \in \mathbb{Z}$ be prime, and $q \nmid n$. Let Q be a prime ideal above q in $\mathbb{Z}[\zeta_n]$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $\sigma(\zeta_n) = \zeta_n^q$. Show that $\sigma(Q) = Q$. (Hint: $f(x^q) \equiv f(x)^q \pmod{q}$ for f a polynomial.)

Solution: Let $\alpha = \sum_{i=0}^{n-1} a_i \zeta_n^i \in Q$, where $a_i \in \mathbb{Z}$. Note that the hint can be extended to $f(x^q) \equiv f(x)^q \pmod{Q}$. Then

$$\begin{aligned}
\sigma(\alpha) &= \sigma\left(\sum_{i=0}^{n-1} a_i \zeta_n^i\right) \\
&= \sum_{i=0}^{n-1} a_i \sigma(\zeta_n^i) \\
&= \sum_{i=0}^{n-1} a_i \zeta_n^{iq} \\
&\equiv \left(\sum_{i=0}^{n-1} a_i \zeta_n^i\right)^q \equiv \alpha^q \pmod{Q}.
\end{aligned}$$

But since $\alpha \in Q$, $\sigma(\alpha) \equiv \alpha^q \equiv 0 \pmod{Q}$, so $\sigma(\alpha) \in Q$ as well. Hence, we have that $\sigma(Q) \subseteq Q$, and because $\sigma(Q)$ is a prime ideal and thus a maximal ideal, $\sigma(Q) = Q$.

Problem 3. Show that $(p) = (1 - \zeta_p)^{p-1}$ in $\mathbb{Z}[\zeta_p]$, where p is a prime, and that $(1 - \zeta_p)$ is a prime ideal in $\mathbb{Z}[\zeta_p]$. (Hint: $(1 - \zeta_p^a) = (1 - \zeta_p)$ for $\gcd(a, p) = 1$.)

Solution: We have the following formula (in ordinary algebraic integers): $(1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1}) = p$. Thus, $(p) = (1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1}) = (1 - \zeta_p)^{p-1}$ (as ideals) as per the hint. Since $ref = p - 1$, (p) can have no more than $p - 1$ prime ideal factors — which are clearly the $p - 1$ copies of $(1 - \zeta_p)$.

Grade obtained: 85%.

Week 13 (16 Nov 2023)

Problem 1. Which cyclotomic fields have only finitely many units? What are these units?

Solution: Dirichlet's unit theorem states the following: The unit group of a number field K is of the form $U = W \times V$, where $W = \mu(\mathcal{O}_K)$ is the multiplicative group of roots of unity in K, and V is a free abelian group of rank $r + s - 1$, where r and $2s$ are the number of real and nonreal embeddings of K into $\mathbb{C}$ respectively. For $n \geq 3$, cyclotomic fields have no real embeddings, so a cyclotomic field $K := \mathbb{Q}(\zeta_n)$ has finitely many units iff W is trivial, i.e., $r + s - 1 = 0$ or $s = 1$. $[K : \mathbb{Q}] = \varphi(n) = 2s$, thus we seek all solutions to $\varphi(n) = 2$: these are $n = 3$ and 4.

These units are then precisely the roots of unity $\mu_n \subset \mathbb{Q}(\zeta_n)$: in the case of $\mathbb{Q}(\zeta_3)$, $\{1, \zeta_3, \zeta_3^2\}$; and in the case of $\mathbb{Q}(\zeta_4)$, $\{1, i, -1, -i\}$.

Problem 2. What are the units in $\mathbb{Q}(\sqrt{-23})$?

Solution: It is known that imaginary quadratic fields have only finitely many units; thus, we seek the roots of unity $\mu(\mathcal{O}_K)$ in $K := \mathbb{Q}(\sqrt{-23})$, i.e., elements $\alpha \in K$ such that $\mathrm{N}(\alpha) = \pm 1$. Since $-23 \equiv 1 \pmod 4$, the algebraic integers of K are of the form $\frac{a+b\sqrt{-23}}{2}$, where $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$. Thus,

$$\begin{aligned} \mathrm{N}\left(\frac{a + b\sqrt{-23}}{2}\right) &= \left(\frac{a + b\sqrt{-23}}{2}\right)\left(\frac{a - b\sqrt{-23}}{2}\right) \\ &= \frac{a^2 + 23b^2}{4} \\ &= \pm 1, \end{aligned}$$

or $a^2 + 23b^2 = \pm 4$. Clearly, any integer $b > 0$ will cause the LHS to exceed 4, so $b = 0$. This leaves us with $a = \pm 2$ as the only solutions, so the only roots of unity are $\frac{a+b\sqrt{-23}}{2} = \frac{\pm 2}{2} = \pm 1$.

Alternatively, let $\pm p \equiv 1 \pmod 4$ be an odd prime, $K = \mathbb{Q}(\sqrt{\pm p})$, and $L = \mathbb{Q}(\zeta_p)$. It is known that $\mathcal{O}_K$ is a subring of $\mathcal{O}_L = \mathbb{Z}[\zeta_p]$, which induces an injective homomorphism (say, ϕ) from the unit group of K to that of L. In fact, since group homomorphisms preserve torsion, any root of unity in K is mapped to a root of unity in L, which all satisfy $\zeta^p = \pm 1_L$. Let ε be a root of unity in K, then $\phi(\varepsilon^p) = \phi(\varepsilon)^p = \pm 1_L = \phi(\pm 1_K)$, so $\varepsilon^p - 1 = 0$ in K (up to a sign).

Let α be algebraic of degree n. If $\alpha \in K$, then $n \leq [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = 2$. Thus, we need only consider elements of degree ≤ 2 satisfying $\varepsilon^p = \pm 1$. However, $x^n - 1 = \prod_{d|n} \Phi_n(x)$, so any element satisfying $\varepsilon^p - 1 = 0$ must have degree dividing p, i.e., 1 or p. Since the only roots of unity of degree 1 over $\mathbb{Q}$ are ± 1, these are precisely the roots of unity in $\mathbb{Q}(\sqrt{\pm p})$. In particular, the units in $\mathbb{Q}(\sqrt{-23})$ are exactly the roots of unity, hence ± 1.

Problem 3. What are the algebraic integers of $\mathbb{Q}(\sqrt{-23})$?

Solution: For $r, s \in \mathbb{Q}$ and $d \equiv 1 \pmod 4$ squarefree, $r + s\sqrt{d}$ is an algebraic integer iff $x^2 - 2rx + r^2 - ds^2$ has integer coefficients. Thus, $r = \frac{a}{2}$ where $a \in \mathbb{Z}$. If $a \equiv 0 \pmod 2$, $r^2 - ds^2 \in \mathbb{Z}$ iff $s \in \mathbb{Z}$. If $a \equiv 1 \pmod 2$, $r^2 - ds^2 \in \mathbb{Z}$ iff $s \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$. This can be summarised as

$$\mathbb{A} \cap \mathbb{Q}(\sqrt{d}) = \left\{ \frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\}.$$

Problem 4. Prove that $(2, (1 + \sqrt{-23})/2)$ is a prime ideal above 2 in $\mathbb{Q}(\sqrt{-23})$.

Solution: Let I be $(2, (1 + \sqrt{-23})/2)$. Since $r \leq ref = 2$, 2 lies under at most two primes in $\mathcal{O}_K$.

Let $J = (2, (1 - \sqrt{-23})/2)$. We see that $IJ = (2)$. Moreover, 2 does not divide $\frac{1+\sqrt{-23}}{2}$: there are no integers a, b such that $\frac{1+\sqrt{-23}}{2} = 2(\frac{a+b\sqrt{-23}}{2}) = a + b\sqrt{-23}$. Hence, $I \neq (2)$; by a similar argument, $J \neq (2)$. Notice that we have exhibited exactly two ideals dividing (2). These must be distinct since 2 is unramified. Hence, I and J are prime ideals.

Problem 5. Show that $(2, (1 + \sqrt{-23})/2)$ is nonprincipal in $\mathbb{Q}(\sqrt{-23})$.

Solution: Note that $\|I\|$ divides $\gcd(\|(2)\|, \|((1 + \sqrt{-23})/2)\|) = \gcd(4, 6) = 2$. Since $\|I\| \neq 1$, $\|I\| = 2$. Suppose $I = (\alpha)$ for some algebraic integer $\alpha = \frac{a+b\sqrt{-23}}{2}$, where $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$. Then since $\|(\alpha)\| = |\mathrm{N}(\alpha)| = \frac{a^2+23b^2}{4} = 2$, we must have $a^2 + 23b^2 = 8$, which has no solutions in integers. Hence, I cannot be principal.

Grade obtained: 85%.