Homework 6

Kevin Guillen

MATH 202 — Algebra III — Spring 2022

Problem 14.2.17 Let K/F be any finite extension and let $\alpha \in K$. Let L be a Galois extension of F containing K and let $H \leqslant \mathrm{Gal}(L/F)$ be the subgroup corresponding to K. Define the norm of α from K to F be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

where the product is taken over all the embeddings of K into an algebraic closure of F (so over a set of coset representatives for H in $\mathrm{Gal}(L/F)$ by the Fundamental Theorem of Galois Theory). This is a product of Galois conjugates of α. In particular, if K/F is Galois this is $\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

Proof. We see that the product of this norm is well defined since K is the fixed field of H, and the elements of a coset $\sigma H \subset \mathrm{Gal}(L/F)$ all correspond to the same embedding of σ. This means then that if I and J were to be two sets of coset representatives of H,

$$\prod_{\sigma \in J} \sigma(\alpha) = \prod_{\sigma \in J} \sigma(\alpha).$$

Next, if J is a set of coset representatives for H, we see that for any $\pi \in \mathrm{Gal}(L/F)$ that πJ is also a complete set of representatives, which we will refer to as M. Meaning then that,

$$\begin{aligned}
\pi N_{K/F}(\alpha) &= \pi \prod_{\sigma \in J} \sigma(\alpha) \\
&= \prod_{\sigma \in J} \pi\sigma(\alpha) \\
&= \prod_{\sigma \in M} \sigma(\alpha) \\
&= N_{K/F}(\alpha).
\end{aligned}$$

Showing us that $N_{K/F}(\alpha)$ lies in F, since it is fixed by $\mathrm{Gal}(L/F)$.

We see through the following that the norm is multiplicative, let $\alpha, \beta \in K$,

$$\begin{aligned}
N_{K/F}(\alpha\beta) &= \prod_{\sigma} \sigma(\alpha\beta) \\
&= \prod_{\sigma} \sigma(\alpha)\sigma(\beta) \\
&= \prod_{\sigma} \sigma(\alpha) \prod_{\sigma} \sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta).
\end{aligned}$$

Now if $K = F(\sqrt{D})$ is a quadratic extension of F, then we'd have that K/F is Galois. In this scenario the only non-identity element of $\mathrm{Gal}(K/F)$ is the map $\sqrt{D} \mapsto -\sqrt{D}$, and therefore ($\alpha \in K$),

$$\begin{aligned} N_{K/F}(\alpha) &= N_{K/F}(a + b\sqrt{D}) && a, b \in F \\ &= (a + b\sqrt{D})(a - b\sqrt{D}) \\ &= a^2 - Db^2 \end{aligned}$$

Let $d = [F(\alpha) : F]$ and $n = [K : F]$, then it is clear that $d \mid n$ since $F \subseteq F(\alpha) \subseteq K$. We have $F \subseteq K \subseteq L$ and since L is Galois over F, we have L is separable over F, therefore K must also be separable over F. Recall that the roots of the minimal polynomials must precisely be the Galois conjugates of α, and m_α doesn't have multiple roots (m_α being the minimal polynomial). We know there must d of them since $\deg(m_\alpha) = d$. We also have that there are n embeddings of K into an algebraic closure of F, and that each of these embeddings sends α to a Galois conjugate, therefore each conjugate appears n/d times in the product of the norm. Let $\{\alpha, \ldots, \alpha_d\}$ be the roots of m_α then we have,

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha) = \left(\prod_{i=1}^{d} \alpha_i \right)^{n/d}.$$

Consider that $a_0 = (-1)^d \prod_{i=1}^{d} \alpha_i$ we have,

$$N_{K/F}(\alpha) = (-1)^n \alpha_0^{n/d}$$

as desired.

$\square$

Problem 14.5.5 Let p be a prime and let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{p-1}$ denote the primitive p^{th} roots of unity. Set $p_n = \varepsilon_1^n + \varepsilon_2^n + \cdots + \varepsilon_{p-1}^n$, the sum of the n^{th} powers of the ε_i. Prove that $p_n = -1$ if p does not divide n and that $p_n = p - 1$ if p does not divide n. [One approach: $p_1 = -1$ from $\varphi_p(x)$; show that p_n is a Galois conjugate of p_1 for p not dividing n, hence is also -1.]

Proof. Because $\varphi_p = x^{p-1} + x^{p-2} + \cdots + 1$ we have $\varphi(\zeta_p) = 0 = p_1 + 1 \implies p_1 = -1$. Recall though that the elements of the Cyclotomic Galois group are defined by $\sigma_a(\zeta_p) = \zeta_p^a$ where $p \nmid a$, therefore we have $\sigma_a(p_1) = p_a$ and so for $p \nmid a$ we have that $p_a = -1$.

In the case that $p \mid a$ we have $\varepsilon_i^a = (\varepsilon_i^p)^m = 1^m = 1 \implies p_a = p - 1$. $\square$

Problem 14.5.10 Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

Proof. We know from the text that the Cyclotomic fields $\mathbb{Q}(\zeta_n)$ are Galois extensions of $\mathbb{Q}$ with abelian Galois groups. If $\mathbb{Q}(\zeta_n)$ were to contain $\mathbb{Q}(\sqrt[3]{2})$ it would have to contain its Galois closure over $\mathbb{Q}$, which is the splitting field of $x^3 - 2$, but that is an extension with Galois group isomorphic to S_3. Therefore by the Fundamental Theorem of Galois Theory, this would imply that the abelian group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ contains a subgroup isomorphic to S_3, which is a contradiction! $\square$

Problem 14.5.11 Prove that the primitive n^{th} roots of unity form a basis over $\mathbb{Q}$ for the cyclotomic field of n^{th} roots of unity if and only if n is squarefree (i.e., n is not divisible by the square of any prime).

Proof. Let p be a prime, and suppose that $p^2 \mid n$. We have then that $\zeta_n^{n/p}$ is a primitive p^{th} root of unity. Which gives us,

$$\sum_{i=0}^{p-1} \zeta_n \zeta_n^{ni/p} = \zeta_n \left(\sum_{i=0}^{p-1} \zeta_n^{ni/p} \right) = \zeta_n 0 = 0$$

and that $\zeta_n \zeta_n^{ni/p} = \zeta_n^{1+ni/p}$ are primitive n^{th} roots of unity for all $0 \leqslant i < p$ since the prime factors of n are factors of n/p. Therefor there are linear dependencies over $\mathbb{Q}$ between the primitive n^{th} roots of unity, so they can't form a basis.

Now suppose the conclusion hold for product of less than x primes and let $n = mp$ for prime p, and m the product of $x-1$ distinct primes. By induction $\left\{ \zeta_p^i \mid 1 \leqslant i \leqslant p,\ (i,p) = 1 \right\}$ is a basis of $\mathbb{Q}(\zeta_p)$ and $\left\{ \zeta_m^j \mid 1 \leqslant j \leqslant m, (j,m) = 1 \right\}$ is a basis of $\mathbb{Q}(\zeta_m)$. Because $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ we have that a basis $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_m, \zeta_p) = \mathbb{Q}(\zeta_n)$ which is

$$\left\{ \zeta_p^i \zeta_m^j \mid 1 \leqslant i \leqslant p, 1 \leqslant j \leqslant m, (j,m) = 1, (i,p) = 1 \right\}.$$

Then by taking mod m and mod p of $mi + pj$ we have that the exponents of $mi + pj$ are relatively prime top n so this basis consist of primitive n^{th} roots of unity. Taking the mods we can again see all these exponents are distinct, so that there are $\varphi(p)\varphi(m) = \varphi(n)$ elements in this basis, meaning it is composed of all the primitive n^{th} roots of unity. $\square$

Problem 14.5.12 Let σ_p denote the Frobenius automorphism $x \mapsto x^p$ of the finite field $\mathbb{F}_q$ of $q = p^n$ elements. Viewing $\mathbb{F}_q$ as a vector space V of dimension n over $\mathbb{F}_p$ we can consider σ_p as a linear transformation σ_p is diagonalizable over $\mathbb{F}_p$ if and only if n divides $p-1$, and is diagonalizable over the algebraic closure of $\mathbb{F}_p$ if and only if $(n,p) = 1$.

Proof. Since for all $x \in \mathbb{F}_{p^n}$, we have $x^{p^n} - x = 0$ we have that σ_p satisfies $x^n - -1$. Since this is a degree n polynomials it is the characteristic polynomial. Now recall that σ_p is diagonalizable if and only if the characteristic polynomial splits completely in $\mathbb{F}_p$.

Now we observe that σ_p is diagonalizable if and only if $\mathbb{F}_p$ contains all the n^{th} roots of unity, if and only if $\mathbb{F}_p^\times$ contains a copy of $\mathbb{Z}/n\mathbb{Z}$. We have then by the Fundamental Theorem of Cyclic Groups this is the case if and only if $n \mid (p-1)$.

The linear transformation is diagonalizable over the closure of $\mathbb{F}_p$ if and only if $x^n - 1$ is separable. This is true if and only if it is relatively prime to its derivative nx^{n-1}, but the this is only true if and only if $nx^{n-1} \neq 0$ and this is true if and only if $p \nmid n$. $\square$

Problem 14.6.2 Determine the Galois groups of the following polynomials

(a) $x^3 - x^2 - 4$

(b) $x^3 - 2x + 4$

(c) $x^3 - x + 1$

(d) $x^3 + x^2 - 2x - 1$

Proof. We know from the textbook that a reducible cubic has trivial Galois group if it is factored as three linear components and has Galois group $\mathbb{Z}_2$ if it is factored as a cubic and a linear polynomial. An irreducible cubic polynomial has Galois group either A_3 or S_3 and it is A_3 if and only if the discriminant $D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ is a square.

(a) We have that $x^3 - x^2 - 4 = (x^2 + x + 2)(x - 2)$ and applying the quadratic formula we see the quadratic has complex roots, so its Galois group is $\mathbb{Z}_2$.

(b) We have $x^3 - 2x + 4 = (x^2 - 2x + 2)(x + 2)$ and the quadratic polynomials has complex roots by the quadratic formula, so like before, its Galois group is $\mathbb{Z}_2$.

(c) The polynomial $x^3 - x + 1$ is irreducible in $\mathbb{Q}$. This is because for $a, b \in \mathbb{Z}$ where $b \neq 0$ and $(a, b) = 1$ and

$$\frac{a^3}{b^3} - \frac{a}{b} + 1 = 0 \implies a^3 = (a - b)b^2$$

meaning that $b^2 \mid a^3$ which contradicts $(a, b) = 1$. We see the discriminant of $x^3 - x + 1$ is $4 - 27 = -23$ which is not a square, so its Galois group is S_3.

(d) We have $x^3 + x^2 - 2x - 1$ to be irreducible in $\mathbb{Q}$ since as before if $(a, b) = 1$ we see if,

$$\frac{a^3}{b^3} + \frac{a^2}{b^2} - \frac{2a}{b} - 1 = 0$$

this would imply $a^3 = (-a^2 + 2ab + b^2)$, which means $b \mid a^3$ which goes against the assumption that a and b are relatively prime.

The discriminant of $x^3 + x^2 - 2x - 1$ is $4 + 32 + 4 - 27 + 36 = 7^2$, which is a square, therefore its Galois group is A_3 $\square$

Problem 14.6.5 Determine the Galois group of $x^4 + 4$

Proof. Let $p(x) = x^4 + 4$ we see that it can be factored into,

$$p(x) = x^4 + 4 = (x^2 - 2x + 4)(x^2 + 2x + 2)$$

which shows us that the roots of $p(x)$ are $\pm 1, \pm i$. Meaning the splitting field is $\mathbb{Q}(i)$, which is of degree 2 over $\mathbb{Q}$. This gives us then that the Galois group of $p(x)$ is cyclic of order 2, which is $\mathbb{Z}_2$. $\square$

Problem 14.6.10 Determine the Galois group of $x^5 + x - 1$

Proof. Let $p(x) = x^5 + x - 1$. We see that $p(x)$ can be factored as,

$$p(x) = x^5 + x - 1 = (x^3 + x^2 - 1)(x^2 - x + 1)$$

We see that the discriminant of $x^2 - x + 1$ is -3 giving us that it is irreducible and its Galois group is simply $\mathbb{Z}_2$. Next we see that $x^3 + x^2 - 1$ is irreducible through mod 2, and its discriminant is -23 so its Galois group is S_3.

Now let K and E be the splitting field of $x^2 - x + 1$ and $x^3 + x^2 - 1$ respectively. Now suppose the intersection between K and E is non-trivial. Because $[K : \mathbb{Q}] = 2$ and $[E : \mathbb{Q}] = 6$ the intersection begin non-trivial would imply $K < E$ and therefore E is an extension of degree 3 on K. This gives us that $\mathrm{Gal}(E/K)$ is some subgroup of $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$ of order 3, and there is a unique subgroup satisfying this, A_3. Giving us $\mathrm{Gal}(E/K) \cong A_3$. This is only possible though if the discriminant of $x^3 + x^2 - 1$ is a square in $K = \mathbb{Q}(i\sqrt{3})$.

Now let $a, b, c, d \in \mathbb{Z}$ and $b, d \neq 0$, suppose then that

$$\left(\frac{a}{b} + \frac{c}{d} i\sqrt{3}\right)^2 = -23$$

for some $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}(i\sqrt{3})$ in lowest terms. This would give us,

$$(ad)^2 - 3(cb)^2 + abcd2i\sqrt{3} = -23$$

so either $a = 0$ or $c = 0$, but both lead to contradiction.

Therefore we have that $K \cap L$ must be trivial, giving us the Galois group to be $\mathbb{Z}_2 \times S_3$. $\square$

Problem 14.6.11 Let F be an extension of $\mathbb{Q}$ of degree 4 that is not Galois over $\mathbb{Q}$. Prove that the Galois closure of F has Galois group either S_4, A_4 or the dihedral group D_8 of order 8. Prove that the Galois group is dihedral if and only if F contains a quadratic extension of $\mathbb{Q}$.

Proof. Say that $E/\mathbb{Q} = \overline{F}$. Now for some $\alpha \in F$ that is a root, we can say that $F = \mathbb{Q}(\alpha)$, and so E is the splitting field of the minimal polynomial of α. We know this polynomial is of degree 4, we know then that $G = \mathrm{Gal}(E/\mathbb{Q})$ is a subgroup of S_4.

Because E has a subfield that is 4th degree in $\mathbb{Q}$, G must have a subgroup of index 4. Since F is given to not be Galois over $\mathbb{Q}$, we have that $|G| > 4$. So we have then that the order of G must be 8, 12, or 24.

If we have the order to be 8, we have $G = D_8$, the only group of order 8 that has a subgroup which is not normal and therefore corresponds to F. If the order were to be 24 we'd have G to be S_4 itself. If the order were to be 12 it is just the only index 2 subgroup of S_4, A_4.

F contains a quadratic extension of $\mathbb{Q}$ if and only if each index 4 subgroup of G is contained in an index 2 subgroup. Notice though that S_4 and A_4 fail this, but each element of D_8 having order 2 is contained in a subgroup of order 4. $\square$