Mathematics W4043 Algebraic Number Theory Assignment # 6

Benjamin Church

Worked With Matthew Lerner-Brecher

February 17, 2018

1. (a) The splitting field of $X^7 - 1$ is the field $\mathbb{Q}(\zeta_7)$ which is a Cyclotomic extension with Galois group $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) = (\mathbb{Z}/7\mathbb{Z})^\times \cong C_6$. Since C_6 is cyclic, it has a unique subgroup of index d for every $d \mid 6$. In particular, there are subgroups corresponding to $d = 1, 2, 3, 6$. Therefore, there is a subfield of index d over $\mathbb{Q}$. Since the fields are unique, the fields of index 1 and 6 must be $\mathbb{Q}$ and $\mathbb{Q}(\zeta_6)$ respectivly. The unique subgroup $C_2 < C_6$ is generated by complex conjugation and its corresponding subfield has index 6 and must be fixed by complex conjugation. By uniqueness, this field is $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ which is real and thus fixed by complex conjugation. Finally, the subgroup $C_3 < C_6$ is generated by the element $\sigma : x \mapsto x^2$ (by unqueness and the fact that σ has order 3) and the corresponding field of order 2 must be fixed under σ. Let $z = \zeta_7 + \zeta_7^2 + \zeta_7^4$ so that $\sigma(z) = \zeta_7^2 + \zeta_7^4 + \zeta_7^8 = \zeta_7 + \zeta_7^2 + \zeta_7^4 = z$. Thus, $\mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$ must be the unique subfield fixed by C_3 and thus has degree 2 over $\mathbb{Q}$.

   (b) By properties of cyclic groups, there is a unique subgroup of $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong C_6$ with index 2, namely, $C_3 < C_6$. By the fundamental theorem of Galois theory, this unique subgroup corresponds to a unique subfield of $\mathbb{Q}(\zeta_7)$ with degree 2 over $\mathbb{Q}$. Call this field $K' = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$ by the above argument. Suppose that a prime $p \in \mathbb{Q}$ does not ramify in K then by the decomposition of the ramification index, $e_{K/L}(\mathfrak{p}) = e_{K/L'}(\beta) e_{K/L'}(\beta')$, we conclude that p cannot ramify in K'. Since $K = \mathbb{Q}(\zeta_7)$ is a cyclotomic field, $\mathcal{O}_K = \mathbb{Z}[\zeta_7]$ and $\mathcal{O}_K / p\mathcal{O}_K \cong \mathbb{Z}[X]/(p, \Phi_7(X)) \cong \mathbb{F}_p[X]/(\Phi_7(X))$. Thus, p is ramified if and only if $\Phi_7(X)$ has a double root in $\mathbb{F}_p$ which can only ocurr if $7 \equiv 0 \pmod{p}$ so $p = 7$. Thus, the only prime that can ramify in K' is 7. Now, K' is a quadratic extension of $\mathbb{Q}$ so it must be $K' = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Q}$. However, p ramifies in $\mathbb{Q}(\sqrt{d})$ if and only if $p \mid d$ therefore, $d = -1$ or ± 7 because d is squarefree and can only be divisible by 7. The only quadratic subfield has a fixed field of order 3 so complex conjugation cannot fix the field so it must be complex. We can exclude $d = -1$ because if $i \in \mathbb{Q}(\zeta_7)$ then the group of roots unity would contain elements of order 4 which is impossible because it is generated by an element of order 7, namely, ζ_7. Therefore, $d = -7$ so $K = \mathbb{Q}(\sqrt{-7})$ and since K' is a complex quadratic extension of $\mathbb{Q}$, $r_1 = 0$ and $r_2 = 1$.

   (c) For the factorization $n = p_1^{k_1} \cdots p_r^{k_r}$ we have $\phi(n) = n \prod\limits_{i=1}^{r} \frac{p_i - 1}{p_i}$ but if $n > 2$ then either some $p_i - 1$ is even or $n = 2^k$ with $k > 1$ so $\phi(n) = 2^{k-1}$ is even. In the first case, $p - 1$ is even and $\prod\limits_{i=1}^{r} p_i$ divides n so $p - 1$ divides $\phi(n)$ so $\phi(n)$ must be even.

Let $K_n = \mathbb{Q}(\zeta_n)$ be the splitting field of $X^n - 1$ with Galois group $Gal(K_n/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$. We write $n = 2^m p_1^{k_1} \cdots p_r^{k_r}$ and use the Chinese Remainder Theorem to conclude that

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/2^m\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times$$

with

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \begin{cases} C_1 & m = 1 \\ C_2 & m = 2 \\ C_2 \times C_{2^{m-2}} & m > 2 \end{cases}$$

and

$$(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times \cong C_{\phi\left(p_i^{k_i}\right)} = C_{p_i^{k_i - 1}(p-1)}$$

Each subfield of degree 2 corresponds uniquely to a subgroup of index 2. Now, we use the fact that, in an abelian group of order a, there is a one-to-one correspondence between subgroups of order b and subgroups of order a/b. Therefore, we classify the subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ of order 2. These each are generated by the distinct elements of order 2. Each even cyclic factor (and every non-trivial cyclic factor here is even) contains a unique element of order 2 and an arbitrary element of order 2 is a product of these. We can have the product of any subset besides the empty product of these elements. Thus, there are $2^c - 1$ elements of order 2 where c is the number of non-trivial cyclic components. Given the above decomposition, we have

$$c = \begin{cases} r & m = 0, 1 \\ r + 1 & m = 2 \\ r + 2 & m > 2 \end{cases}$$

These elements uniquely correspond to subgroups of index 2 each corresponding to a subfield of degree 2. By a similar argument to (b), we know that the subfield corresponding to the order two element contained in the cyclic factor with prime p is $\mathbb{Q}(\sqrt{\pm p})$. The sign is determined as follows, the unique group of index 2 in $C_{p^{k-1}(p-1)}$ is $C_{p^k \frac{p-1}{2}}$ which is cyclic so, if $\frac{p-1}{2}$ is even, it must contain an element of order 2. However, there is a unique element of order 2 given by $\sigma : \zeta_p \mapsto \zeta_p^{-1}$ which acts as complex conjugation. Therefore, if $p \equiv 1 \pmod 4$ then the quadratic subfield is fixed by σ and is thus real. However, if $p \equiv 3 \pmod 4$ then $C_{p^k \frac{p-1}{2}}$ has odd order so it cannot contain σ and thus its corresponding subfield is not fixed by complex conjugation so the subfield is complex. In summary, the unique quadratic subfield corresponding to the order two element in each odd prime cyclic factor is $\mathbb{Q}(\sqrt{\chi(p) \cdot p})$ where χ is the Dirichlet character modulo 4. Now, the product elements correspond to the quadratic fields generated by the products of these elements (which are included in the field by multiplicative closure), i.e. $\mathbb{Q}(\sqrt{\chi(p_1 \cdots p_s) \cdot p_1 \cdots p_s})$ for s distinct primes dividing n. Also, if $m = 1$ we get no further elements but if $m = 1$ then we also have $\mathbb{Q}(i)$ because $\zeta_n^{n/4} = i$. If $m > 2$ then $8 \mid n$ so we also have the quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i\sqrt{2})$ because $\zeta_n^{n/8} = \frac{1}{\sqrt{2}}(1 + i)$ and $i = \zeta_n^{n/4}$. We can also use these elements to make product fields. Finally, the $2^c - 1$ quadratic subfields are,

$$\mathbb{Q}(\sqrt{\chi(p_1 \cdots p_s) \cdot p_1 \cdots p_s})$$

for s distinct primes dividing n and if n is divisible by four, we also have the fields,

$$\mathbb{Q}(\sqrt{-\chi(p_1 \cdots p_s) \cdot p_1 \cdots p_s})$$

and if n is divisible by 8 add to those the fields,

$$\mathbb{Q}(\sqrt{2\chi(p_1 \cdots p_s) \cdot p_1 \cdots p_s})$$

and

$$\mathbb{Q}(\sqrt{-2\chi(p_1 \cdots p_s) \cdot p_1 \cdots p_s})$$

Let $n = p_1 p_2$ where p_1 and p_2 are distinct primes. If both primes are odd, we have the quadratic subfields $\mathbb{Q}(\sqrt{\chi(p_1)p_1})$, $\mathbb{Q}(\sqrt{\chi(p_2)p_2})$, and $\mathbb{Q}(\sqrt{\chi(p_1p_2)p_1p_2})$. If one prime is even, WLOG let $p_2 = 2$, then we only have the quadratic subfield $\mathbb{Q}(\sqrt{\chi(p_1)p_1})$. The embedding numbers are $r_1 = 2, r_2 = 0$ for a real quadratic field and $r_1 = 0, r_2 = 1$ for a complex quadratic field. The subfield $\mathbb{Q}(\sqrt{\chi(p_1)p_1})$ is real if $\chi(p_1) = 1$ i.e. if $p_1 \equiv 1 \pmod 4$ and complex if $\chi(p_1) = -1$ i.e. if $p_1 \equiv 3 \pmod 4$. The same condition holds generally for any of these fields.

2. Let $K = \mathbb{Q}(\sqrt{d})$ then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4 \end{cases}$$

For $d \not\equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ so we can take the basis $\{1, \sqrt{d}\}$ and then, by exercise 6.15, the discriminant, Δ, is given by the square of the determinant of $A_{ij} = \sigma_i(x_j)$ with $\sigma_1 = \text{id}$ and $\sigma_2 : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ and x_j ranging over the basis. This matrix is,

$$A = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}$$

which has determinant, $\det A = -2\sqrt{d}$ so $\Delta = 4d$. Now, consider the alternative basis $\{1 + \sqrt{d}, 1 + 2\sqrt{d}\}$. This set is also a basis because,

$$(1 + 2\sqrt{d}) - (1 + \sqrt{d}) = \sqrt{d} \quad \text{and} \quad 2 \cdot (1 + \sqrt{d}) - (1 + 2\sqrt{d}) = 1$$

The marix is then given by,

$$A = \begin{pmatrix} 1 + \sqrt{d} & 1 + 2\sqrt{d} \\ 1 - \sqrt{d} & 1 - 2\sqrt{d} \end{pmatrix}$$

which has determinant, $\det A = (1 - \sqrt{d} - 2d) - (1 + \sqrt{d} - 2d) = -2\sqrt{d}$ so $\Delta = 4d$.

For $d \equiv 1 \pmod 4$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathbb{Z} \oplus \mathbb{Z}(\frac{1+\sqrt{d}}{2})$ so we can take the basis $\{1, \frac{1+\sqrt{d}}{2}\}$ and then, by exercise 6.15, the discriminant, Δ, is given by the square of the determinant of $A_{ij} = \sigma_i(x_j)$ with $\sigma_1 = \text{id}$ and $\sigma_2 : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ and x_j ranging over the basis. This matrix is,

$$A = \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}$$

which has determinant, $\det A = \frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2} = -\sqrt{d}$ so $\Delta = d$. Now, consider the alternative basis $\{\frac{1-\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}\}$. This set is also a basis because,

$$\frac{1-\sqrt{d}}{2} + \frac{1+\sqrt{d}}{2} = 1 \quad \text{and} \quad \frac{1+\sqrt{d}}{2} - \frac{1-\sqrt{d}}{2} = \sqrt{d}$$

The marix is then given by,

$$A = \begin{pmatrix} \frac{1-\sqrt{d}}{2} & \frac{1+\sqrt{d}}{2} \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}$$

with determinant, $\det A = \frac{1}{4}(1-\sqrt{d})^2 - \frac{1}{4}(1+\sqrt{d})^2 = \frac{1}{4}(1-2\sqrt{d}+d) - \frac{1}{4}(1+2\sqrt{d}+d) = -\sqrt{d}$ so $\Delta = d$.

3. Let $p \in \mathbb{Q}$ be prime and let $r \in \mathbb{N}$. Then let $K = \mathbb{Q}(\zeta)$ where ζ_{p^r} is a primitive p^r root of unity which is the splitting field of

$$F(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = \prod_{p \nmid i}^{p^r} (X - \zeta^i)$$

(a) Let $r = 1$. Then

$$F(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1 = \prod_{i=1}^{p-1} (X - \zeta_p^i)$$

Now, by exercise 6.15, the discriminant of the basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ is given by

$$D(1, \zeta, \zeta^2, \ldots, \zeta^{p-2}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{\mathbb{Q}}^{K}\left(F'(\zeta)\right)$$

because F is the minimal polynomial of ζ. Now, $n = \deg F = p - 1$ and,

$$F'(X) = \frac{pX^{p-1}(X-1) - (X^p - 1)}{(X-1)^2}$$

therefore,

$$F'(\zeta) = \frac{p\zeta^{p-1}(\zeta - 1) - (\zeta^p - 1)}{(\zeta - 1)^2} = \frac{p\zeta^{p-1}}{\zeta - 1}$$

so taking the norm,

$$\mathrm{N}_{\mathbb{Q}}^{K}\left(F'(\zeta)\right) = \mathrm{N}_{\mathbb{Q}}^{K}(p)\, \mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta^{p-1}\right) \mathrm{N}_{\mathbb{Q}}^{K}(\zeta - 1)^{-1}$$

each of these terms can be easily calculated. Since $p \in \mathbb{Q}$, p is fixed by every Galois automorphism so $\mathrm{N}_{\mathbb{Q}}^{K}(p) = \prod_{\sigma \in G} \sigma(p) = p^{p-1}$. Also, because $p - 1$ is even,

$$\mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta^{p-1}\right) = \mathrm{N}_{\mathbb{Q}}^{K}(\zeta) = (-1)^{p-1} = 1$$

because

$$F(0) = 1 = \prod_{i=1}^{p-1}(-\zeta^i) = (-1)^{p-1} \prod_{\sigma \in G} \sigma(\zeta)) = (-1)^{p-1} \mathrm{N}_{\mathbb{Q}}^{K}(\zeta)$$

Finally,

$$F(1) = p = \prod_{i=1}^{p-1}(1-\zeta^i) = (-1)^{p-1}\prod_{\sigma\in G}\sigma(\zeta-1)) = (-1)^{p-1}\mathrm{N}_{\mathbb{Q}}^{K}(\zeta-1)$$

so $\mathrm{N}_{\mathbb{Q}}^{K}(\zeta-1) = p$ and therefore, $\mathrm{N}_{\mathbb{Q}}^{K}(F'(\zeta)) = p^{p-2}$ so $D(1,\zeta,\ldots,\zeta^{p-2}) = \pm p^{p-2}$

(b)

$$D(1,\zeta,\zeta^2,\ldots,\zeta^{p-2}) = (-1)^{\frac{n(n-1)}{2}}\mathrm{N}_{\mathbb{Q}}^{K}(F'(\zeta)) = (-1)^{\frac{(p-1)(p-2)}{2}}p^{p-2}$$

since $p-2$ is odd, the exponent is even iff $4 \mid p-1$. Thus,

$$D(1,\zeta,\zeta^2,\ldots,\zeta^{p-2}) = \begin{cases} +p^{p-2} & p \equiv 1 \pmod 4 \\ -p^{p-2} & p \equiv 3 \pmod 4 \end{cases}$$

(c) For general r,

$$F'(X) = \frac{p^r X^{p^r-1}(X^{p^{r-1}}-1) - p^{r-1}X^{p^{r-1}-1}(X^{p^r}-1)}{(X^{p^{r-1}}-1)^2}$$

Now, by exercise 6.15, the discriminant of the basis $\{1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^r)-1}\}$ is given by

$$D(1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^r)-1}) = (-1)^{\frac{n(n-1)}{2}}\mathrm{N}_{\mathbb{Q}}^{K}(F'(\zeta))$$

because F is the minimal polynomial of ζ. In particular,

$$F'(\zeta) = \frac{p^r\zeta^{p^r-1}(\zeta^{p^{r-1}}-1) - p^{r-1}\zeta^{p^{r-1}-1}(\zeta^{p^r}-1)}{(\zeta^{p^{r-1}}-1)^2} = \frac{p^r\zeta^{p^r-1}}{\zeta^{p^{r-1}}-1}$$

so taking the norm,

$$\mathrm{N}_{\mathbb{Q}}^{K}(F'(\zeta)) = \mathrm{N}_{\mathbb{Q}}^{K}(p^r)\,\mathrm{N}_{\mathbb{Q}}^{K}(\zeta^{p^r-1})\,\mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta^{p^{r-1}}-1\right)^{-1}$$

Since $p^r \in \mathbb{Q}$, p^r is fixed by every Galois automorphism so $\mathrm{N}_{\mathbb{Q}}^{K}(p) = \prod_{\sigma\in G}\sigma(p^r) = (p^r)^{\phi(p^r)}$. Also, because $\phi(p^r)$ is even, $\mathrm{N}_{\mathbb{Q}}^{K}(\zeta^{p-1}) = \mathrm{N}_{\mathbb{Q}}^{K}(\zeta) = (-1)^{\phi(p^r)} = 1$. This holds because,

$$F(0) = 1 = \prod_{p\nmid i}^{p^r}(-\zeta^i) = (-1)^{\phi(p^r)}\prod_{\sigma\in G}\sigma(\zeta)) = (-1)^{\phi(p^r)}\mathrm{N}_{\mathbb{Q}}^{K}(\zeta)$$

However, $\zeta_p = \zeta^{p^{r-1}}$ is a primitive p^{th} root of unit so,

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}}^{K}\left(\zeta^{p^{r-1}}-1\right) &= \prod_{\sigma\in G}\sigma(\zeta^{p^{r-1}}-1) = \prod_{p\nmid i}^{p^r}(\zeta_p^i-1) = \prod_{k=0}^{p^{r-1}-1}\prod_{i=1}^{p-1}(\zeta_p^{kp+i}-1) \\ &= \prod_{k=0}^{p^{r-1}-1}\prod_{i=1}^{p-1}(\zeta_p^i-1) = \prod_{k=0}^{p^{r-1}-1}p = p^{p^{r-1}}\end{aligned}$$

Therefore,

$$\mathrm{N}_{\mathbb{Q}}^{K}(F'(\zeta)) = p^{r\phi(p^r)-p^{r-1}} = p^{p^{r-1}(pr-r-1)}$$

because $\phi(p^r) = p^{r-1}(p-1)$ so we conclude that

$$D(1,\zeta,\zeta^2,\ldots,\zeta^{\phi(p^r)-1}) = \pm p^{p^{r-1}(pr-r-1)}$$