Homework 5
Algebra

Joshua Ruiter

February 21, 2018

Proposition 0.1 (Exercise 9)**.** *Let K/k be a finite separable extension, with $[K : k] = p$ for a prime p and $K = k(\theta)$. Let $\sigma_1, \ldots, \sigma_p$ be the distinct embeddings of K into $\overline{k}$, and let $\theta_1 = \sigma_1(\theta), \ldots, \theta_p = \sigma_p(\theta)$ be the conjugates of θ. Assume $\theta = \theta_1$, and suppose $\theta_2 \in K$. Then K/k is Galois and cyclic.*

Proof. Assume K is embedded in an algebraic closure $\overline{k}$, and let L be the splitting field of $\operatorname{Irr}(\theta, k)$ in $\overline{k}$, that is, $L = k(\theta_1, \ldots, \theta_p)$. Since K/k is separable, so is L/k, so L/k is Galois. Furthermore, L/k is finite.

We know that the degree of $\operatorname{Irr}(\theta, k)$ divides $[L : k]$, and that $[L : k] = |\operatorname{Gal}(L/k)|$. Since $\deg \operatorname{Irr}(\theta, k) = p$, we get that p divides $|\operatorname{Gal}(L/k)|$. Since this is a finite group, by Cauchy's Theorem, $|\operatorname{Gal}(L/k)|$ has an element of order p, call it σ. Since $\sigma \in G = \operatorname{Gal}(L/k)$, for any k we have $\sigma^k(\theta) = \theta_i$ for some i, so

$$\{\theta, \sigma(\theta), \sigma^2(\theta), \ldots, \sigma^{p-1}(\theta)\}$$

has p distinct elements. It is also a subset of $\{\theta_1, \ldots, \theta_p\}$, so they must be equal as sets.

$$\{\theta, \sigma(\theta), \sigma^2(\theta), \ldots, \sigma^{p-1}(\theta)\} = \{\theta_1, \ldots, \theta_p\}$$

Thus $\sigma^m(\theta) = \theta_2$ for some m. Note that since $K = k(\theta)$ and $\sigma^m(k) \subset k$ and $\sigma^m(\theta) = \theta_2 \in K$ (by hypothesis), we have $(\sigma^m)^k(K) \subset K$ for any k. Since p is prime, m is relatively prime to p, so σ^m is also of order p, so

$$\{\theta, \sigma^m(\theta), (\sigma^m)^2(\theta), \ldots, (\sigma^m)^{p-1}(\theta)\}$$

is a set with p distinct elements. Thus

$$\{\theta, \sigma^m(\theta), (\sigma^m)^2(\theta), \ldots, (\sigma^m)^{p-1}(\theta)\} = \{\theta_1, \ldots, \theta_p\}$$

so we have $\theta_1, \ldots, \theta_p \in \sigma^m(K) \subset K$. Thus $L = k(\theta_1, \ldots, \theta_p) \subset K$, so K is the splitting field for $\operatorname{Irr}(\theta, k)$. Thus K/k is normal, so it is Galois. Since $\operatorname{Gal}(K/k)$ has order $[K : k] = p$ and has an element of order p, it is cyclic. □

Proposition 0.2 (Exercise 15)**.** *Let K/k be a Galois extension and let F be an intermediate field, $k \subset F \subset K$. Let $G = \operatorname{Gal}(K/k)$, and define*

$$H = \{\sigma \in G : \sigma(F) \subset F\}$$

Let $A = \operatorname{Gal}(K/F)$. Then $H = N_A$ (the normalizer of A in G.)

Proof. First we show that $H \subset N_A$. We need to show that for $\sigma \in H$, we have $\sigma^{-1} A \sigma = A$, which we will show by showing that the sets include both ways. First we show $\sigma^{-1} A \sigma \subset A$. Let $\sigma \in H$ and $\tau \in A$. Then $\tau|_F = \mathrm{Id}_F$, so if $x \in F$, then

$$\sigma^{-1}\tau\sigma(x) = \sigma^{-1}(\tau(\sigma(x)) = \sigma^{-1}(\sigma(x)) = x$$

(because $\sigma(x) \in x$), so $\sigma^{-1}\tau\sigma|_F = \mathrm{Id}_F$, so $\sigma^{-1}\tau\sigma \in A$. Since $\sigma^{-1} \in H$ as well, we also have $\sigma A \sigma^{-1} \subset A$.

Now we show $A \subset \sigma^{-1} A \sigma$ for $\sigma \in H$. Let $\tau \in A$. By the above, $\sigma A \sigma^{-1} \subset A$, so $\sigma\tau\sigma^{-1} \in A$. Then since $\sigma^{-1} A \sigma \subset A$, we have

$$\sigma^{-1}(\sigma\tau\sigma^{-1})\sigma \in \sigma^{-1} A \sigma \implies \tau \in \sigma^{-1} A \sigma$$

Thus $A \subset \sigma^{-1} A \sigma$. This completes the argument that $H \subset N_A$.

Now we show $N_A \subset H$. Let $\sigma \in N_A$. We just need to show that $\sigma(F) \subset F$. Using the previous part, $\sigma^{-1}\tau\sigma \in A$, so $\sigma^{-1}\tau\sigma|_F = \mathrm{Id}_F$, so $\tau\sigma|_F = \sigma_F$. Thus for $x \in F$,

$$\tau(\sigma(x)) = \sigma(x)$$

which says that $\sigma(x)$ is in the fixed field of A. The fixed field of A is precisely F, so $\sigma(x) \in F$. Thus $N_A \subset H$. Together with the opposite inclusion, this shows $N_A = H$. ☐

I have placed exercise 18a after 18b since I use the result from 18b in the arguments for 18a.

Proposition 0.3 (for Exercise 18b)**.** *Let $m \in \mathbb{N}$. Then $\phi(m) = 2$ if and only if $m = 3, 4, 6$.*

Proof. It is straightforward to check that $\phi(m) = 2$ for $m = 3, 4, 6$ and no other small values of m. We claim that for $m > 6$, $\phi(m) > 2$. We can write m as a product of primes,

$$m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

Then by the multiplicative property of ϕ,

$$\phi(m) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \dots \phi(p_n^{k_n})$$

If any $p_i \geq 5$, then $\phi(m) \geq p_i - 1 \geq 4 > 2$, so we can assume m is only divisible by the primes 2 and 3, so $m = 2^{k_1} 3^{k_2}$. Then using the formula for $\phi(p^k)$,

$$\phi(m) = \phi(2^{k_1})\phi(3^{k_2}) = (2^{k_1-1})(2-1)(3^{k_2-1})(3-1) = 2(2^{k_1-1}3^{k_2-1}) \geq 2$$

This is equal to 2 precisely when $k_1 = 1$ and $k_2 = 1$, and strictly larger for all other k_1, k_2. Thus for $m > 6$, we have $\phi(m) > 2$. ☐

Proposition 0.4 (Exercise 18b)**.** *A primitive mth root of unity has degree 2 over $\mathbb{Q}$ if and only if $m = 3, 4, 6$.*

Proof. By Theorem 3.1 in Lang, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ where ϕ is the Euler totient function. One can check by counting that $\phi(m) = 2$ for $m = 3, 4, 6$ and not for $m = 1, 5$. By the previous lemma, $\phi(m) > 2$ for $m > 6$, so these are the only possible values of m. ☐

Lemma 0.5 (for Exericse 18a)**.** *Let p, q be distinct primes. Then $\mathbb{Q}(\sqrt{p}) \cap \mathbb{Q}(\sqrt{q}) = \mathbb{Q}$.*

Proof. Suppose the intersection is not empty. Then $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$, so

$$\sqrt{q} = a + b\sqrt{p}$$

for some $a, b \in \mathbb{Q}$. Then

$$q = (a + b\sqrt{p})^2 = a^2 + 2ab\sqrt{p} + b^2 p$$

But q is an integer, and $2ab\sqrt{p}$ is not an integer, so this is a contradiction. □

Proposition 0.6 (Exercise 18a)**.** *The only roots of unity in $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-5})$ are ± 1. $\mathbb{Q}(i)$ contains all 4th roots of unity, and $\mathbb{Q}(\sqrt{-3})$ contains all 6th roots of unity.*

Proof. Both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are contained in $\mathbb{R}$, so they can only contain roots of unity that lie in $\mathbb{R}$. The only roots of unity in $\mathbb{R}$ are ± 1, so those are the only roots of unity in $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$.

Consider a general quadratic extension $\mathbb{Q}(\alpha)$ for some α be algebraic over $\mathbb{Q}$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, and suppose $\mathbb{Q}(\alpha)$ contains an nth root of unity ζ. Then we have a tower $\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\alpha)$, and by the tower law, $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ must be 1 or 2. If it is one, then $\zeta \in \mathbb{Q}$, so $\zeta = \pm 1$. If it is 2, then by 18a, $n = 3, 4$, or 6. We can enumerate the 3rd, 4th, and 6th roots of unity in $\mathbb{C}$:

$$\text{3rd roots: } 1, \frac{-1 \pm \sqrt{-3}}{2} \qquad \text{4th roots: } \pm 1, \pm i \qquad \text{6th roots: } \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}$$

Now consider $\alpha = \sqrt{-2}$ and $\alpha = \sqrt{-5}$. (These are in fact quadratic extensions, with irreducible polynomials $x^2 + 2$ and $x^2 + 5$ respectively.) By the previous general argument, the only possible roots of unity in these extensions are 3rd, 4th, or 6th roots. We claim that neither $\mathbb{Q}(\sqrt{-2})$ nor $\mathbb{Q}(\sqrt{-5})$ contains any 3rd, 4th, or 6th root of unity except for ± 1. It is sufficient to show that neither contains $\sqrt{-3}$, because of the expressions for 3rd and 6th roots of unity above. Using the previous lemma with primes -2,-3, and -2,-5 says that $\mathbb{Q}(\sqrt{-2}) \cap \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}$ and $\mathbb{Q}(\sqrt{-5}) \cap \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}$. □

Lemma 0.7 (for Exercise 19a)**.** *Let k be a field with algebraic closure $\overline{k}$, and let $\alpha \in \overline{k}$ be algebraic over k. Let $f(x) = \mathrm{Irr}(\alpha, k)$. Let $a, b \in k$ with $a \neq 0$. Then*

$$\mathrm{Irr}(a\alpha + b, k) = \imath c f\left(\frac{1}{a}(x - b)\right)$$

where c is the leading coefficient of $f\left(\frac{1}{a}(x - b)\right)$.

Proof. We check that $a\alpha + b$ is a root of $f\left(\frac{1}{a}(x - b)\right)$.

$$f\left(\frac{1}{a}(a\alpha + b - b)\right) = f\left(\frac{1}{a}(a\alpha)\right) = f(\alpha) = 0$$

Since f is irreducible, so is this linear transoformation of f. The adjustment by $\frac{1}{c}$ forces the leading coefficient to be 1. Thus this transformed f is the irreducible polynomial of $a\alpha + b$. □

Lemma 0.8 (for Exercise 19)**.** *Let $n \in \mathbb{N}$. If $n = p^r$ for some prime p, then $\Phi_n(1) = p$. If n is not a prime power, then $\Phi_n(1) = 1$.*

Proof. First suppose that n is a prime power. Then

$$\Phi_n(x) = \Phi_{p^r}(x) = \Phi_p\left(x^{p^{r-1}}\right) = \left(x^{p^{r-1}}\right)^{p-1} + \left(x^{p^{r-1}}\right)^{p-2} + \ldots + 1$$

There are p terms, and plugging in 1 for x makes each term one, so $\Phi_n(1) = p$. Now suppose n is not a prime power. We will proceed by induction on n. For $n = 6$,

$$\Phi_6(x) = x^2 - x + 1$$

so the result holds in the base case. Assume that $\Phi_j(1) = 1$ for every non-prime power up to $n - 1$, and factor n into prime powers as $n = p_1^{k_1} \ldots p_m^{k_m}$. We know that

$$\Phi_n(x) = \prod_{d|n} \Phi_d(x)$$

so

$$1 + x + \ldots + x^{n-1} = \prod_{d|n, d\neq 1} \Phi_d(x) = \Phi_n(x) \prod_{d|n, d\neq 1, d\neq n} \Phi_d(x)$$

Plugging in $x = 1$ gives

$$n = \Phi_n(1) \prod_{d|n, d\neq 1, d\neq n} \Phi_d(1)$$

By induction hypothesis, $\Phi_d(1) = 1$ for d not equal to a prime power, and $\Phi_{p_i^{k_i}}(1) = p_i$. For each p_i, there are exactly k_i times that $d = p_i^r$ in the product, so

$$\prod_{d|n, d\neq 1, d\neq n} \Phi_d(1) = p_1^{k_1} \ldots p_m^{k_m} = n$$

Thus

$$n = \Phi_n(1) n \implies \Phi_n(1) = \frac{n}{n} = 1$$

This completes the induction. □

Lemma 0.9 (for Exercise 19)**.** *Let ϕ be the Euler phi function. Then $\phi(n)$ is even for $n \geq 3$.*

Proof. If n is a prime power, then we know that

$$\phi(n) = \phi(p^r) = p^{r-1}(p-1)$$

If p is odd, then $p-1$ is even so $\phi(n)$ is even. If p is even (i.e. $p = 2$), then $r > 1$ since $n \geq 3$, so p^{r-1} is even. Thus $\phi(n)$ is even for n a prime power. If n is not a prime power, then we can write n as a product of prime powers $p_1^{k_1} \ldots p_m^{k_m}$. Then by the multiplicative property,

$$\phi(n) = \phi(p_1^{k_1}) \ldots \phi(p_m^{k_m})$$

and one of the p_i must be at least 3 since $n \geq 3$. Thus $\phi(n)$ is even by the previous argument. □

Proposition 0.10 (Exercise 19a)**.** *Let p be a prime, and let $n = p^r$ for $r \in \mathbb{N}$. Let ζ be a primitive nth root of unity, and let $K = \mathbb{Q}(\zeta)$. Then $N_{K/\mathbb{Q}}(1-\zeta) = p$.*

Proof. We know that the irreducible polynomial of ζ over $\mathbb{Q}$ is $\Phi_n(x)$ (Lang pg 279), so using the previous lemma, the irreducible polynomial of $1-\zeta$ over $\mathbb{Q}$ is $\Phi_n(1-x)$. By Theorem 5.1 (Lang pg 285),

$$N_{K/\mathbb{Q}}(1-\zeta) = (-1)^{\phi(n)} a_0$$

where a_0 is the constant term of $\Phi_n(1-x)$. In our case, $n = p^r$, so by the previous lemma, $\Phi_n(1) = p$, that is, the constant term a_0 of $\Phi_n(1-x)$ is p. By another lemma, $\phi(n)$ is even as long as $n \geq 3$. (If $n = 2$, then the result is trivial since $\zeta = -1$.) Thus

$$N_{K/\mathbb{Q}}(1-\zeta) = p$$

□

Proposition 0.11 (Exercise 19b)**.** *Let n be divisible by at least two primes, and let ζ be a primitive nth root of unity, and let $K = \mathbb{Q}(\zeta)$. Then $N_{K/\mathbb{Q}}(1-\zeta) = 1$.*

Proof. As in part (a), the irreducible polynomial of $(1-\zeta)$ is $\Phi_n(1-x)$, and $N_{K/\mathbb{Q}}(1-\zeta)$ is $(-1)^{\phi(n)} a_0$ where a_0 is the constant term of $\Phi_n(1-x)$. Since n is divisible by at least two primes, $n \geq 3$ so $\phi(n)$ is even. As shown in previous lemma, for n divisible by at least two primes, $\Phi_n(1) = 1$, that is, $a_0 = 1$. Thus

$$N_{K/\mathbb{Q}}(1-\zeta) = a_0 = 1$$

□

Lemma 0.12 (for Exercise 21a)**.** *Let $n \in \mathbb{N}$. The discriminant of $x^n - 1$ is $\pm n^n$.*

Proposition 0.13 (Exercise 21a)**.** *Let $a \in \mathbb{Z}$, $a \neq 0$, let p be a prime, and let $n \in \mathbb{Z}^+$ such that p does not divide n. Then p divides $\Phi_n(a)$ if and only if a has period n in $(\mathbb{Z}/p\mathbb{Z})^*$.*

Proof. Suppose a has period n in $(\mathbb{Z}/p\mathbb{Z})^*$. Then $a^n \equiv 1 \bmod p$, and $a^k \not\equiv \bmod p$ for $k < n$ Then $p | a^n - 1$. Since

$$a^n - 1 = \prod_{d|n, d \leq n} \Phi_d(a) = \Phi_n(a) \prod_{d|n, d<n} \Phi_d(a)$$

If p does not divide $\Phi_n(a)$, then it must divide some other $\Phi_d(a)$. But

$$a^d - 1 = \prod_{k|d} \Phi_d(a)$$

so $\Phi_d(a) | a^d - 1$, so then p divides $a^d - 1$, and then $a^d \equiv 1 \bmod p$ with $d < n$. This is a contradiction since n is the order of a. Thus we conclude that p does not divide any $\Phi_d(a)$ for $d < n$, so $p | \Phi_n(a)$.

Now suppose that p divides $\Phi_n(a)$. Let k be the multiplicative order of $a \bmod p$, and suppose $k \neq n$. By the previous direction $p | \Phi_k(a)$. Then $p | a^n - 1$ and $p | a^k - 1$, so $a^n \equiv$

$a^k \equiv 1 \bmod p$. Since k is the order, $k|n$. Let R be the resultant of $\Phi_n(x)$ and $\Phi_k(x)$. By the remark on page 202 of Lang, R can be written as

$$R(x) = f(x)\Phi_n(x) + g(x)\Phi_n(x)$$

where $f, g \in \mathbb{Z}[x]$. Since p divides both $\Phi_n(a)$ and $\Phi_k(a)$, p must divide $R(a)$. By Proposition 8.5 (Lang pg 204), $R(x)$ divides the discriminant of any common multiple of $\Phi_n(x)$ and $\Phi_k(x)$. In particular, since $k|n$, $x^n - 1$ is a common multiple of $\Phi_n(x)$ and $\Phi_k(x)$. The discriminant of $x^n - 1$ is $\pm n^n$. We have that p divides $R(a)$, which divides $\pm n^n$, so p must divide n. This is a contradiction, since p does not divide n (by hypothesis). Thus the order of a mod p must not be k for $k \neq n$, so it must be precisely n. □

Lemma 0.14 (for Exercise 23a). *Let $(G, \times)$ be an abelian group with elements $x_1, \dots, x_t$ with finite orders $n_1, \dots, n_t$. Then the order of $x_1 \dots x_t$ is $\operatorname{lcm}(n_1, \dots, n_t)$.*

Proof. We may assume that no x_i is the identity. For $i \neq j$, since x_i, x_j have relatively prime orders, x_i cannot be a power of x_j, since all powers of x_j have order that divides the order of x_j (using Lagrange's Theorem). As a consequence, the cyclic subgroups $\langle x_i \rangle$ and $\langle x_j \rangle$ intersect only in the identity.

In the case $t = 1$ there is nothing to prove. Suppose $t = 2$, and let k be the order of $x_1 x_2$. Then

$$(x_1 x_2)^k = 1 \implies x_1^k = x_2^{-k}$$

Since $\langle x_i \rangle \cap \langle x_j \rangle = \{1\}$, this implies $x_1^k = x_2^{-k} = 1$, so k is a multiple of both n_1 and n_2. By definition, k is minimal, so $k = \operatorname{lcm}(n_1, n_2)$.

Now we prove the general statement by induction. Suppose it holds true up to t, and we have $x_1, \dots, x_{t+1}$ with orders $n_1, \dots, n_{t+1}$. By inductive hypothesis, the order of $x_1 \dots x_t$ is $\operatorname{lcm}(n_1, \dots, n_t)$. Then by the case $t = 2$, the order of $(x_1 \dots x_t)x_{t+1}$ is $\operatorname{lcm}(\operatorname{lcm}(n_1, \dots, n_t), n_{t+1})$. Since lcm is associative, this is equal to $\operatorname{lcm}(n_1, \dots, n_t, n_{t+1})$, so the induction is complete. □

Lemma 0.15 (for Exercise 23a). *Let $(G, \times)$ be an abelian group with elements $x_1, \dots, x_t$ of (finite) orders $n_1, \dots, n_t \in \mathbb{N}$ respectively. Suppose that $\gcd(n_i, n_j) = 1$ for all i, j. Then the order of $x_1 \dots x_t$ is $n_1 \dots n_t$.*

Proof. By Lemma 0.14, the order of $x_1, \dots, x_t$ is $\operatorname{lcm}(n_1, \dots, n_t)$. Since $\gcd(n_i, n_j) = 1$, in particular we have $\gcd(n_1, \dots, n_t) = 1$. We have the equality

$$\Big(\gcd(n_1, \dots, n_t)\Big)\Big(\operatorname{lcm}(n_1, \dots, n_t)\Big) = n_1 \dots n_t$$

Since the gcd is one, we get $\operatorname{lcm}(n_1, \dots, n_t) = n_1 \dots n_t$. □

Lemma 0.16 (for Exercise 23a). *Let $n_1, \dots, n_t$ be pairwise relatively prime positive integers. Then*

$$(\mathbb{Z}/(n_1 \dots n_t)\mathbb{Z})^* \cong \prod_{i=1}^{t} (\mathbb{Z}/n_i\mathbb{Z})^*$$

Proof. See Lang page 95. □

Lemma 0.17 (for Exercise 23a)**.** *Let $n_1, \dots, n_t$ be pairwise relatively prime positive integers, and for each i let ζ_i be a primitive n_ith root of unity. Define $\zeta = \prod_{i=1}^t \zeta_i$. Then ζ is a primitive $\left(\prod_{i=1}^t n_i\right)$-th root of unity, and*

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \prod_{i=1}^{t} (\mathbb{Z}/n_i\mathbb{Z})^*$$

Proof. Apply the previous lemma to the group of nonzero complex numbers under multiplication, with $x_i = \zeta_i$. Each ζ_i has order n_i, and the n_i are all pairwise relatively prime. Lemma 0.15 allows us to conclude that ζ has order $\prod_{i=1}^t n_i$, so ζ is a primitive root of unity of that order. Then by Theorem 3.1 in Lang,

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/(n_1 \dots n_t)\mathbb{Z})^*$$

which by Lemma 0.16 is isomorphic to $\prod_{i=1}^t (\mathbb{Z}/n_i\mathbb{Z})^*$. □

Proposition 0.18 (Exercise 23a)**.** *Let G be a finite abelian group. Then there exists an abelian extension of $\mathbb{Q}$ with Galois group G.*

Proof. We can write G as a product of cyclic groups.

$$G \cong \prod_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z}$$

By the result in 23(b), for each $i = 1, \dots, t$ there are infinitely may primes p so that $p \equiv 1 \bmod n_i$. Choose p_1 so that $p_1 \equiv 1 \bmod n_1$. Then choose p_2 from the infinite set of primes $\equiv 1 \bmod n_2$. Inductively, choose p_i so that $p_1, \dots, p_i$ are distinct primes and $p_i \equiv 1 \bmod n_i$. Thus we have distinct primes $p_1, \dots, p_t$ so that $p_i \equiv 1 \bmod n_i$.

Since $p_i \equiv 1 \bmod n_i$, we have $n_i | p_i - 1$, so there exist m_i so that $m_i n_i = p_i - 1$. Since $(\mathbb{Z}/p_i\mathbb{Z})^*$ is a cyclic group of order $p_i - 1$, there is a unique subgroup $H_i \subset (\mathbb{Z}/p_i\mathbb{Z})^*$ of order $m_i = \frac{p_i - 1}{n_i}$. Then $(\mathbb{Z}/p_i\mathbb{Z})^*/H_i$ is a cyclic group of order $\frac{p_i-1}{m_i} = n_i$, so $(\mathbb{Z}/p_i\mathbb{Z})^*/H_i \cong \mathbb{Z}/n_i\mathbb{Z}$. Define $H = \prod_{i=1}^t H_i$. Then we can rewrite G as

$$G \cong \prod_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z} \cong \prod_{i=1}^{t} (\mathbb{Z}/p_i\mathbb{Z})^*/H_i \cong \frac{\prod_{i=1}^t (\mathbb{Z}/p_i\mathbb{Z})^*}{\prod_{i=1}^t H_i} \cong \frac{\prod_{i=1}^t (\mathbb{Z}/p_i\mathbb{Z})^*}{H}$$

For each i, let ζ_i be a primitive p_ith root of unity, and define $\zeta = \prod_{i=1}^t \zeta_i$. Then by Lemma 0.17,

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \prod_{i=1}^{t} (\mathbb{Z}/p_i\mathbb{Z})^*$$

Let K be the fixed field of H. Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a product of abelian groups it is abelian, so H is a normal subgroup. Thus $K/\mathbb{Q}$ is Galois, and by the funamental theorem, it has Galois group

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \Big(\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\Big)/H \cong \frac{\prod_{i=1}^t (\mathbb{Z}/p_i\mathbb{Z})^*}{\prod_{i=1}^t H_i} \cong G$$

Thus K is the desired abelian extension field of $\mathbb{Q}$ with Galois group G. □