Math 129 HW 8

Bryden Cais

April 17, 2002

1

1. Marcus # 33

   (a) Let $m \equiv 2$ or $3 \mod 4$ be a positive squarefree integer. We know that the ring of integers of $K = \mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\sqrt{m}]$. Moreover, since roots of unity of K are just ± 1 (since $K \subset \mathbb{R}$), we know that every unit in K is $\pm u^h$ for some $h \in \mathbb{Z}$ where u is a fundamental unit. Denote by $\bar{s}$ the image of $s \in K$ under the generator of $\mathrm{Gal}(K/\mathbb{Q})$. Let b be the least positive integer such that $mb^2 \pm 1 = a^2$ for some positive integer a. We know that there must be such a b since every unit $x + y\sqrt{m}$ satisfies $my^2 \pm 1 = x^2$. Write $u = c + d\sqrt{m}$ and without loss of generality, assume that $c, d > 0$. Certainly $c \neq 0$ since then the square of u is rational. Then we can at any rate choose $c > 0$ by multiplying u by -1 if necessary, and notice that for any unit z, $\bar{z}$ is also a unit so that $\bar{z} = \pm u^h$ for some h which implies that $z = \pm \bar{u}^h$ whence $\bar{u}$ is also a fundamental unit. Therefore, if $u = c + d\sqrt{m}$ with $c > 0$ and $d < 0$ replace u by $\bar{u}$. Since $a + b\sqrt{m}$ is a unit, we write $a + b\sqrt{m} = \pm(c + d\sqrt{m})^r$ for some $r \in \mathbb{Z}$. Notice first that the $+$ sign must hold above since a, b, c, d are all positive. Moreover, because a, b, c, d are positive, $c + d\sqrt{m}, a + b\sqrt{m}$ are both greater than 1, so that $r \geq 1$. Since we have assumed b to be minimal, we have $d \geq b$. If $d \geq b + 1$ then $c^2 \geq md^2 - 1 \geq mb^2 + (2b+1)m - 1 > mb^2 + 1 \geq a^2$ since $b \neq 0$, obviously, and $m \equiv 2$ or $3 \mod 4$ is at least 2. Therefore, if $d > b$ then $c > a$ so that $a + b\sqrt{m} < c + d\sqrt{m}$, which is impossible since $r \geq 1$. Therefore we conclude that $b = d$ so that a^2, c^2 are equal or differ by 2 (since $mb^2 \pm 1 = a^2, mb^2 \pm 1 = c^2$). But no two squares differ by 2 so that $a = c$ and $r = 1$ and $a + b\sqrt{m}$ is a fundamental unit.

   (b) The argument is virtually identical to before. We know that the ring of integers of $K = \mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. As before, the roots of unity of K are just ± 1 and every unit in K is $\pm u^h$ for some $h \in \mathbb{Z}$ where u is a fundamental unit. Denote by $\bar{s}$ the image of $s \in K$ under the generator of $\mathrm{Gal}(K/\mathbb{Q})$. Let b be the least positive integer such that $mb^2 \pm 4 = a^2$ for some positive integer a. We know that there must be such a b since every unit $(x + y\sqrt{m})/2$ satisfies $my^2 \pm 4 = x^2$. Write $u = (c + d\sqrt{m})/2$ and without loss of generality, assume that $c, d > 0$. The argumant is identical to that above. Since $(a + b\sqrt{m})/2$ is a unit, we write $(a + b\sqrt{m})/2 = \pm((c + d\sqrt{m})/2)^r$ for some $r \in \mathbb{Z}$. Again, the $+$ sign must hold above since a, b, c, d are all positive. Moreover, because a, b, c, d are positive, $a \equiv b, c \equiv d \mod 2$, and $m > 1, d, b \neq 0$, the numbers $(c+d\sqrt{m})/2, (a+b\sqrt{m})/2$ are both greater than 1, so that $r \geq 1$. Since we have assumed b to be minimal, we have $d \geq b$. If $d \geq b+1$ then $c^2 \geq md^2 - 4 \geq mb^2 + (2b+1)m - 4 > mb^2 + 4 \geq a^2$ since $b \neq 0$, obviously, and $m \equiv 1 \mod 4$ is at least 5. Therefore, if $d > b$ then $c > a$ so that $a + b\sqrt{m} < c + d\sqrt{m}$, which is impossible since $r \geq 1$. We conclude that $b = d$ so that a^2, c^2 are equal or they differ by 8. If they differ by 8 then one of a, c is 1 and the other is 3. Since we are supposing that $(a + b\sqrt{m})/2 = ((c + d\sqrt{m})/2)^r$ with $r \geq 1$ and $b = d$ we must have $c = 1$ and $a = 3$, whence $b = d = 1$ and $m = 5$, and indeed $((1 + \sqrt{5})/2)^2 = (3 + \sqrt{5})/2$. Except in this case, we therefore obtain, as above, $b = d, c = a$ so that u is a fundamental unit. The procedure in genreal, as the above example indicates, is to minimize b first and then minimize a.

(c) Applying this procedure to the integers $5, 6, 7$ we find that fundamental units for $\mathbb{Z}[\frac{1+\sqrt{5}}{2}], \mathbb{Z}[\sqrt{6}], \mathbb{Z}[\sqrt{7}]$ are, respectively,

$$\begin{aligned} u_5 &= \frac{1+\sqrt{5}}{2} \\ u_6 &= 5 + 2\sqrt{6} \\ u_7 &= 8 + 3\sqrt{7}. \end{aligned}$$

2

1. Marcus # 43

(a) Let τ be the automorphism of K given by complex conjugation, and let $H = \langle \tau \rangle$. If τ is trivial on K then $\#H = 1$, otherwise τ has order 2 and $\#H = 2$. Clearly we have $K \cap \mathbb{R} = K^H$. The Galois corespondence then gives $[K : K \cap \mathbb{R}] = \#H$ so that K has degree 1 or 2 over $K \cap \mathbb{R}$.

(b) Let $\sigma : K \cap \mathbb{R} \to \mathbb{C}$ be an embedding. Then since K/Q is normal, σ extends to an automorphism $\tilde{\sigma} : K \to K$ whose restriction to $K \cap \mathbb{R}$ is σ. If σ is a real embedding, $\sigma(K \cap \mathbb{R}) \subset \mathbb{R}$ so that $\tilde{\sigma}(K \cap \mathbb{R}) \subset K \cap \mathbb{R}$, that is, $\sigma : K \cap \mathbb{R} \to K \cap \mathbb{R}$ is an automorphism of $K \cap \mathbb{R}$. If $K \cap \mathbb{R}$ has no non–real embeddings in $\mathbb{C}$ then every embedding of $K \cap \mathbb{R}$ is an automorphism of $K \cap \mathbb{R}$ so that $K \cap \mathbb{R}$ is a normal extension of $\mathbb{Q}$. Conversely, is σ is not a real embedding, then $\sigma(K \cap \mathbb{R}) \not\subset K \cap \mathbb{R}$ so that $K \cap \mathbb{R}/Q$ is not normal.

(c) Notice that complex conjugation τ is in the center of $G = \mathrm{Gal}(K/\mathbb{Q})$ if and only if $\langle \tau \rangle = H$ is normal in G. By the Galois correspondence, $H \triangleleft G$ if and only if $K \cap \mathbb{R}/\mathbb{Q}$ is a normal extension with Galois group G/H. By part b, $K \cap \mathbb{R}/\mathbb{Q}$ is a normal extension if and only if there are no non–real embeddings of $K \cap \mathbb{R}$. If $K = K \cap \mathbb{R}$ then $\tau = 1$ is trivial and hence in the center. In this case, $U = U \cap \mathbb{R}$ since K is real and hence $U/U \cap \mathbb{R}$ is finite. Now suppose that $K \neq K \cap \mathbb{R}$. Then $\#H = 2$. Let $r, 2s$ be the number of real and non–real embeddings of K in $\mathbb{C}$. Similarly, let $u, 2v$ be the number of real and non–real embeddings of $K \cap \mathbb{R}$. Then we know that

$$\begin{aligned} U &\simeq C \times \mathbb{Z}^{r+s-1} \\ U \cap \mathbb{R} &\simeq \{\pm 1\} \times \mathbb{Z}^{u+v-1}, \end{aligned}$$

where C is a cyclic group. Furthermore, we have the relations $r+2s = [K : \mathbb{Q}] = n$ and $u + 2v = [K \cap \mathbb{R} : \mathbb{Q}] = n/2$. Since we have supposed that $K \neq K \cap \mathbb{R}$, it must be that K has no real embeddings. Therefore $r = 0, s = n/2$. Now if there are no non–real embeddings of $K \cap \mathbb{R}$ then $v = 0$ and $u = n/2$. It follows that $U \simeq C \times \mathbb{Z}^{n/2-1}$ and $U \cap \mathbb{R} \simeq \{\pm 1\} \times \mathbb{Z}^{n/2-1}$ so that $U/U \cap \mathbb{R} \simeq C/\{\pm 1\} = \{\text{Roots of unity in } K\}/\{\pm 1\}$ is finite. Conversely, if $U/U \cap \mathbb{R}$ is finite then $r + s = u + v$. If in fact $U = U \cap \mathbb{R}$ then $r = u, s = v$ and complex conjugation is trivial. Otherwise, we may assume $K \neq K \cap \mathbb{R}$ so that $r = 0$ as before, $s = n/2$ and $u + 2v = n/2$. This gives two equations in two unknowns with solution $u = n/2, v = 0$, i.e. $K \cap \mathbb{R}$ has no non–real embeddings. Thus we conclude that $U/U \cap \mathbb{R}$ is finite if and only if complex conjugation is in the center of G.

2. Marcus # 45 Let $K/\mathbb{Q}$ be abelian and let $u \in \mathcal{O}_K$ be a unit. If K is real then obviously every unit is the product of a real unit and a root of unity. So assume that K is not real. Denote complex conjugation by $s \mapsto \bar{s}$ and put $v = u/\bar{u}$. Since $K/\mathbb{Q}$ is abelian, complex conjugation commutes with every element of $\mathrm{Gal}(K/\mathbb{Q})$ so that every Galois conjugate of $u/\bar{u}$ has absolute value 1. We showed on an earlier problem set (and will

give the idea again in the next problem) that this implies that v is a root of unity in K. Therefore, write

$$u = \bar{u}\zeta.$$

Noe either $\zeta^{1/2} \in K$ or it is in a degree 2 extension of K. We can write $u\zeta^{-1/2} = \bar{u}\zeta 1/2$ so that $u\zeta{-}1/2$ is real. Thus we can write u as a real unit times a root of unity where the factors are in K or a degree 2 extension of K.

3. Marcus # 46

   (a) For an odd prime p let $\omega = e^{2\pi i/p}$ and put $R = \mathbb{Z}[\omega]$. Let $u \in R$ be a unit. Consider

$$v = \frac{u}{\bar{u}}.$$

Clearly, $|v| = 1$. Moreover, the Galois conjugates of v are v^i for $1 \leq i \leq p-1$ so that $|\sigma(v)| = |v^i| = 1$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. We showed on an earlier problem set that this implies that v is a root of unity (recall the argument: $|\sigma(v^n)| = 1$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and n, but $\mathbb{Z}[\omega]$ can only contain finitely many such algebraic integers since they are the roots of monic irreducible polynomials of bounded degree and bounded coefficients. This implies $v^n = v^m$ for some $m \neq n$). Since v is a root of unity in $\mathbb{Z}[\omega]$, we may write $v = \pm\omega^k$ for some k. We now claim that the $+$ sign holds. Suppose not. Then $u/\bar{u} = -\omega^k$ whence $u^p = -\bar{u^p}$. Now write

$$u = a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}$$

with $a_i \in \mathbb{Z}$. Since $x \mapsto x^p$ is the familiar Frobenius automorphism, we see that $u^p \equiv a_0 + a_1 + \cdots + a_{p-2} \mod p$. We then also have $\bar{u^p} \equiv a_0 + a_1 + \cdots + a_{p-2} \mod p$ so that $\bar{u^p} \equiv u^p \mod p$. Since we are supposing that $\bar{u^p} \equiv -u^p \mod p$, we must have $u^p \equiv 0 \mod p$ since p is odd. Since u is a unit, this is a contradiction. Thus we have $u = \bar{u}\omega^k$. Now choose j so that $2j \equiv k \mod p$. Then we have

$$\begin{aligned} u\omega^{-j} &= \bar{u}\omega^j \\ &= \overline{u\omega^{-j}} \end{aligned}$$

so that $u\omega^{-j} \in \mathbb{R}$. Therefore, $u = \omega^k \cdot u\omega^{-k}$ is the product of a root of unity in R and a real unit.

(b) We showed in part 1 of this question that $U/U \cap \mathbb{R} \simeq C/\{\pm 1\}$ where C is the group of roots of unity in R. In the case $R = \mathbb{Z}[\omega]$, we find that $C = \pm\langle\omega\rangle$, so that

$$U/U \cap \mathbb{R} \simeq \langle\omega\rangle.$$

where U is the group of units in $\mathbb{Z}[\omega]$. Moreover, $\mathbb{Z}[\omega + \omega^{-1}] = \mathbb{Z}[\omega] \cap \mathbb{R}$ since $\mathbb{Q}(\omega + \omega^{-1})$ is the fixed field of complex conjugation. Therefore, the group of units U' in $\mathbb{Z}[\omega + \omega^{-1}]$ is $U \cap \mathbb{R}$. Piecing the information together, we see that $U \simeq \langle\omega\rangle \times U'$.

4. Marcus # 48

(a) Let $\omega = e^{2\pi i/m}$ and set $\alpha = e^{\pi i/m}$. We have

$$\begin{aligned} 1 - \omega^k &= e^{\pi i k/m}\left(e^{-\pi i k/m} - e^{\pi i k/m}\right) \\ &= -2i\alpha^k \frac{e^{\pi i k/m} - e^{-\pi i k/m}}{2i} \\ &= -2i\alpha^k \sin(k\pi/m) \end{aligned}$$

for any $k \in \mathbb{Z}$. Therefore, we conclude that

$$\frac{1-\omega^k}{1-\omega} = \alpha^{k-1}\frac{\sin(k\pi/m)}{\sin(\pi/m)}.$$

(b) If k is odd then $k-1$ is even to that $\alpha^{k-1} = \omega^{(k-1)/2}$. If k is even then we are supposing that m must be odd so that $-\alpha^{k-1} = \alpha^{m+k-1} = \omega(m+k-1)/2$ since $\alpha^m = -1$ and $m+k-1$ is even. Thus, in any case, as long as m, k are not both even $\alpha^k = \pm\omega^h$ for some $h \in \mathbb{Z}$.

(c) If $(k, m) = 1$ then certainly k, m are not both even. Therefore, by parts a and b we have

$$u_k = \frac{\sin(\pi k/m)}{\sin(\pi/m)} = \pm\omega^h \frac{1-\omega^k}{1-\omega}.$$

Again, if $(k, m) = 1$ then the Galois conjugates of ω^k are the same as the Galois conjugates of ω. Therefore,

$$\begin{aligned} \mathrm{N}(u_k) &= \pm\,\mathrm{N}(\omega)\,\mathrm{N}\left(\frac{1-\omega^k}{1-\omega}\right) \\ &= 1, \end{aligned}$$

so that u_k is a unit.

3

1. (a) We have $\pi i(a) = Sa \cap K$. Obviously $a \in Sa \cap K$. Suppose now that $x \in Sa \cap K$. Then $x \in Sa$ and $x \in K$. Thus we can write $x = s\alpha$ for $s \in S$ and $\alpha \in K$. Then $s = x/\alpha \in K$ so that $s \in S \cap K = R$. Therefore $x \in Ra = a$. Thus, $Sa \cap K = a$.

   (b) No, π is not a group homomorphism. For consider a prime P of K ramified in L (We know such a prime exists for any nontrivial extension L/K). Then write $P = QQ_1$ where Q is prime. Then $\pi(Q) = P$ and $\pi(Q_1) \supset P$. But $\pi(QQ_1) = \pi(P) = P$ which is not equal to $\pi(Q)\pi(Q_1) = PP'$ where $P' \supset P$ is clearly not all of R.

2. (a) Marcus # 15

   i. Let $K \subset L \subset M$ be fields and let Q be a prime of M. Let T, S, R denote the rings of integers pf M, L, K respectively. Then

   $$\mathrm{N}_{M/K}(Q) = P^{f(Q|P)}$$

   by definition. Letting Q_L be the unique prime in L below Q, we have $f(Q|P) = f(Q|Q_L)f(Q_L|P)$ which enables us to write

   $$\begin{aligned} \mathrm{N}_{M/K}(Q) &= (P^{f(Q|Q_L)})^{f(Q_L|P)} \\ &= \mathrm{N}_{\mathrm{L/K}}(P^{f(Q|Q_L)}) \\ &= \mathrm{N}_{\mathrm{L/K}}\,\mathrm{N}_{M/L}(P), \end{aligned}$$

   where we have used the multiplicitive extension of N in the second line. Now extending this result multiplicitively to all ideals $I \subset T$ we see that $\mathrm{N}_{M/K}(I) = \mathrm{N}_{\mathrm{L/K}}\,\mathrm{N}_{M/L}(I)$.

   ii. Let $\alpha \in L$ be nonzero. We now show that $\mathrm{N}_{\mathrm{L/K}}(\alpha S)$ is the principal ideal in R generated by the element $\mathrm{N}_{\mathrm{L/K}}(\alpha)$. Let M be the normal closure of L/K. Then by the first part, we have $\mathrm{N}_{M/K}(\alpha T) = \mathrm{N}_{\mathrm{L/K}}\,\mathrm{N}_{M/L}(\alpha T)$. Since M/L is a normal extension, we already know (see Marcus ex. # 14) that $\mathrm{N}_{M/L}(\alpha T)$ is the S ideal generated by the element $\mathrm{N}_{M/L}(\alpha) = \alpha^{[M:L]}$ since $\alpha \in L$. Therefore

   $$\begin{aligned} \mathrm{N}_{\mathrm{L/K}}\,\mathrm{N}_{M/L}(\alpha T) &= \mathrm{N}_{\mathrm{L/K}}(\alpha^{[M:L]}S) \\ &= \mathrm{N}_{\mathrm{L/K}}((\alpha S)^{[M:L]}) \\ &= \mathrm{N}_{\mathrm{L/K}}(\alpha S)^{[M:L]}. \end{aligned}$$

On the other hand, since M/K is Galois,

$$\begin{aligned}
\mathrm{N}_{M/K}(\alpha T) &= \mathrm{N}_{M/K}(\alpha)R \\
&= \mathrm{N}_{\mathrm{L/K}}\,\mathrm{N}_{M/L}(\alpha)R \\
&= \mathrm{N}_{\mathrm{L/K}}(\alpha^{[M:L]})R \\
&= \mathrm{N}_{\mathrm{L/K}}(\alpha)^{[M:L]}R \\
&= (\mathrm{N}_{\mathrm{L/K}}(\alpha)R)^{[M:L]},
\end{aligned}$$

so that $\mathrm{N}_{\mathrm{L/K}}(\alpha S)^{[M:L]} = (\mathrm{N}_{\mathrm{L/K}}(\alpha)R)^{[M:L]}$, from which we conclude that $\mathrm{N}_{\mathrm{L/K}}(\alpha S) = \mathrm{N}_{\mathrm{L/K}}(\alpha)R$.

iii. Now let $K = \mathbb{Q}$, and let Q be a prime in L with $p \in \mathbb{Z}$ the unique primebelow. In this case we have

$$\|Q\| = |S/Q|,$$

which is a finite field of characteristic p. Since it is an extension of degree $f(Q|p)$ of $\mathbb{F}_p$, we conclude that $\|Q\| = p^{f(Q|P)}$. On the other hand, we have shown that $\mathrm{N}_{L/\mathbb{Q}}(Q) = p^{f(Q|P)}$ is the principal ideal of $\mathbb{Z}$ generated by $p^{f(Q|p)}$. Putting things together, we see that $\mathrm{N}_{L/\mathbb{Q}}(Q)$ is the principal ideal in $\mathbb{Z}$ generated by the number $\|Q\|$. Using the fact that $\|IJ\| = \|I\|\|J\|$ for any ideals I, J and that $\mathrm{N}_{L/\mathbb{Q}}(IJ) = \mathrm{N}_{L/\mathbb{Q}}(I)\,\mathrm{N}_{L/\mathbb{Q}}(J)$, we see that $\mathrm{N}_{L/\mathbb{Q}}(I)$ is the principal ideal in $\mathbb{Z}$ generated by $\|I\|$ for any ideal $I \subset S$.

(b) Since $\mathrm{N}_{\mathrm{L/K}}$ is multiplicitive, it is enough to show the result when $a = P$ is prime. We have $i(P) = SP = Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$ so that

$$\begin{aligned}
\mathrm{N}_{\mathrm{L/K}} \circ i(P) &= \prod_{j=1}^{r} \mathrm{N}_{\mathrm{L/K}}(Q_i)^{e_i} \\
&= \prod_{j=1}^{r} \P^{f(Q_i|P)e_i} \\
&= P^{\sum_{i=1}^{r} f(Q_i|P)e_i} \\
&= P^{[L:K]}.
\end{aligned}$$

(c) Marcus # 16.

i. Let $\phi : G(S) \to G(R)$ be the map taking any ideal in a given class C and sending C to the class of $\mathrm{N}_{\mathrm{L/K}}(I)$. This is well defined because if $[I] = [J]$

then $I = \alpha J$ for some $\alpha \in L$ whence $\mathrm{N_{L/K}}(I) = \mathrm{N_{L/K}}(alpha)\,\mathrm{N_{L/K}}(J)$, that is $[\mathrm{N_{L/K}}(I)] = [\mathrm{N_{L/K}}(J)]$ since $\mathrm{N_{L/K}}(\alpha) \in K$. That ϕ is a homomorphism follows immediately from the multiplicitivity of $\mathrm{N_{L/K}}$.

ii. Let Q be a prime lying over the prime P and let d_Q, d_P be the orders of the classes of Q, P in $\mathrm{Cl}(S), \mathrm{Cl}(R)$ respectively. Then we have $\mathrm{N_{L/K}}(Q) = P^{f(Q|P)}$. Since $[Q]^{d_Q} = 1$ and ϕ is a homomorphism we have $[\phi(Q)^{d_Q}] = [P^{d_Q f(Q|P)}] = [P]^{d_Q f(Q|P)} = 1$ so that $d_P | d_Q f(Q|P)$.

(d) Suppose that $[L : K]$ is prime to $\#\,\mathrm{Cl}(K)$. Let p be a prime dividing $\#\,\mathrm{Cl}(K)$. Then $\mathrm{Cl}(K)$ contains an element of order p, say P_p. If $p | f(Q|P_p)$ for every prime Q over P_p then the formula $[L : K] = \sum_{i=1}^{r} e(Q|P) f(Q|P)$ tells us that $p | [L : K]$. Thus, if $p \not| [L : K]$ then $p \not| f(Q|P)$ for some Q over P. Therefore, by part b above, $p | d_Q$. Since d_Q is the order of an element of $\mathrm{Cl}(L)$, we see that $d_Q | \#\,\mathrm{Cl}(L)$ and hence $p |\,\mathrm{Cl}(L)$. Thus every prime divisor of $\mathrm{Cl}(K)$ divides $\mathrm{Cl}(L)$ when $[L : K]$ and $\#\,\mathrm{Cl}(K)$ are relatively prime.

(e) Marcus # 17. Let $K = \mathbb{Q}(\sqrt{-23})$, $L = \mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/23}$. Set $R = \mathcal{O}_K$, let $P = (2, \frac{1+\sqrt{-23}}{2})$ be a prime over 2 (in fact $2 = P\bar{P}$), and let Q be a prime of $S = \mathbb{Z}[\omega]$ lying over P.

i. Since $\mathrm{disc}(L) = \pm 23^h$ for some integer h, we see that $2 \not| \mathrm{disc}(L)$. We know that $f(Q|2)$ is the order of $2 \mod 23$. This must be a factor of 22. Since $2^{11} = 2048 = 23 \cdot 89 + 1$, we see that $f(Q|2) = f$ (since $L/\mathbb{Q}$ is Galois) is 11. On the other hand, $f(Q|2) = f(Q|P)f(P|2)$ and since $2 = P\bar{P}$ is totally split in K, we have $f(P|2) = 1$ and therefore $f(Q|P) = 11$. Again, L/K is Galois so that $e(Q|P)f(Q|P)d = [L : K] = 11$. But $f(Q|P) = 11$, which forces $d = e(Q|P) = 1$, so that P is inert in L.

ii. Notice that $\mathrm{N}(\frac{-3+\sqrt{-23}}{2}) = 2^3 = \mathrm{N}(P^3)$. It is not difficult to see that the principal ideals generated by $\frac{-3+\sqrt{-23}}{2}, \frac{-3-\sqrt{-23}}{2}$ are relatively prime, for if I divides both of them, then $-3 \in I$ and $\sqrt{-23} \in I$ so that $\mathrm{N}(I) |\,\mathrm{N}(3) = 9$ and $\mathrm{N}(I) |\,\mathrm{N}(\sqrt{-23}) = -23$ whence $\mathrm{N}(I) = 1$. Therefore, we see that $P^3 = (\frac{-3+\sqrt{-23}}{2})$ or $(\frac{-3-\sqrt{-23}}{2})$ and $\bar{P}^3$ is the other ideal. At any rate, P^3 is principal. If P were principal, say $P = (\alpha)$ then we would have $P = (a + b\sqrt{-23})/2$ for some $a, b \in \mathbb{Z}$ of the same parity. In this case, we have

$$\mathrm{N}(P) = \frac{a^2 + 23b^2}{4} = 2,$$

so that $a^2 + 23b^2 = 8$. This is clearly impossible.

iii. By # 16b, we have $d_P | d_Q f(Q|P)$, where d_P, d_Q are the orders of P, Q respectively in their respective class groups. We know that $d_P = 3$ and $f(Q|P) = 11$. Since $(3, 11) = 1$, we then have $3 | d_Q$ so that Q is not principal.

iv. We have seen that $2 = QQ^{'}$ where $Q, Q^{'}$ are not principal. Suppose that $2 = \alpha\beta$ with $\alpha, \beta \in S$. Then $Q|(\alpha\beta)$ so that $Q|(\alpha)$ or $Q|(\beta)$. If it happens that Q divides one of $(\alpha), (\beta)$ and $Q^{'}$ divides the other, then without loss of generality we write $(\alpha) = Q\dashv$ and $(\beta) = Q^{'}\lfloor$ for ideals $\dashv, \lfloor$. Moreover, since $\alpha\beta = 2$ and $QQ^{'} = 2$ we see that $\dashv\lfloor = 1$. But this implies that $\dashv = \lfloor = (1)$, so that $(\alpha) = Q$. But (α) is principal and Q is not, a contradiction. Therefore, both $Q, Q^{'}$ divide one of α, β. Without loss of generality assume that they divide α. Then $2|\alpha$ and since $\alpha\beta = 2$, we see that β is a unit.

3.

4

1. Marcus # 5. Let K, L be number fields with L/K normal and $\mathrm{Gal}(L/K) = G$, and let P be a prime of K. By "intermediate field" we mean a field $F \neq K, L$ with $K \subset F \subset L$.

   (a) Suppose that P is inert in L. In this case, $f = \#G$ and $e = d = 1$. Since $[L^D : K] = d$ and $[L : L^I] = e$, we see that $L^D = K$ and $L^I = L$ so that $I = \{1\}$ and $D = G$. Since D/I is cyclic (generated by the Frobenius automorphism), we see that $G = D/I$ is cyclic.

   (b) Suppose that P is totally ramified in every intermediate field but not in L. If $I \neq \{1\}$ then in particular P is totally ramified in L^I. Therefore, since $e(Q^I|P) = 1$ where Q^I is any prime of L^I over P, we see that $[L^I : K] = e(Q^I|P) = 1$ whence $L^I = K$ and $I = G$. Therefore, $[L : L^I] = e(Q|P) = [L : K]$ so that P is totally ramified in L also. Therefore, $I = \{1\}$ and $e(Q|P) = [L : L^I] = 1$. Since $e(Q|P) = e(Q|Q^H)e(Q^H|P)$ for any subgroup H of G, we find that $e(Q^H|P) = 1$ for every subgroup. Thus, if G has any nontrivial subgroups H then P is unramified in the intermediate field L^H, contradicting our assumption, so that there can be no intermediate fields F such that $L \subset F \subset L$ with $F \neq K, F \neq L$. It follows that the order of G is prime since if $d|\#G$ then we have a subgroup of G of order d and hence an intermediate field. But if $\#G$ is prime, then G is cyclic of prime order.

   (c) Suppose that every intermediate field contains a unique prime over P but L does not. If $D \neq \{1\}$ then in particular we have a unique prime Q over P in L^D. But

$e(Q^D|P) = f(Q^D|P) = 1$ so that $[L^D : K] = e(Q^D|P)f(Q^D|P)d = d$ whence $L^D = K$ and $D = G$. Therefore, $[L : L^D] = e(Q|P)f(Q|P) = [L : K]$ where Q is any prime of L over P. But this implies that there is a unique prime in L over P. Therefore, $D = \{1\}$ and $e(Q|P)f(Q|P) = [L : L^D] = 1$ so that $e(Q|P) = f(Q|P) = 1$. As above, by the multiplicitivity of e, f we see that $e(Q^H|P) = f(Q^H|P) = 1$ for any subgroup H of G. Thus, if G has any nontrivial subgroups H then P does not have a unique prime over it in the intermediate field L^H, contradicting our assumption, so that there can be no intermediate fields F such that $L \subset F \subset L$ and $F \neq K, F \neq L$. It follows as above that G is cyclic of prime order.

(d) Suppose that P is unramified in every intermediate field F but ramified in L. Since L^I is the largest intermediate field in which P is unramified, we see that L^I contains every intermediate field of L/K. Moreover, since P is ramified in L, $L \neq L^I$ so that I is not trivial. The Galois correspondence then tells us that every nontrivial subgroup H of G contains I. The group I is then the unique smallest nontrivial subgroup of G. It is smallest because it is contained in every subgroup of G and it is unique because if J were another such group, we have $\#J = \#I$ and $I \subset J$ which implies $I = J$. Moreover, we see that $I \lhd G$ since for any $g \in G$ the group gIg^{-1} has the same size as I and must contain I since it is a nontrivial subgroup of G, so that $gIg^{-1} = I$ for any $g \in G$. Now since I has no nontrivial subgroups (if J were a sungroup of I, it would be a subgroup of G and would then contain I), we see that I must have prime order for otherwise it would have a nontrivial (proper) Sylow subgroup. Now let $\#I = p$ and suppose that $q|\#G$ for some prime q. The G contains an element of order q and hence a subgroup of order q. Since this subgroup is nontrivial, it has I as a subgroup so that $p|q$ implying that $p = q$. Therefore, G has prime power order. Finally, cince the center of a p–group is nontrivial, we see that I is contained in the center of G.

(e) Suppose that P splits completely in every intermediate field but not in L. Since L^D is the largest intermediate field in which P splits completely, we see that L^D contains every intermediate field of L/K. Moreover, since P does not split completely in L, $L \neq L^D$ so that D is not trivial. The Galois correspondence then tells us that every nontrivial subgroup H of G contains D. The group D is then the unique smallest nontrivial subgroup of G. It is smallest because it is contained in every subgroup of G and it is unique because if J were another such group, we have $\#J = \#D$ and $D \subset J$ which implies $D = J$. Moreover, we see that $D \lhd G$ since for any $g \in G$ the group gDg^{-1} has the same size as D and must contain D since it is a nontrivial subgroup of G, so that $gDg^{-1} = D$ for any $g \in G$. Now since D has no nontrivial subgroups (if J were a sungroup of D, it would be a subgroup of G and would then contain D), we see that D must have prime order for otherwise it would have a nontrivial (proper) Sylow subgroup. Now let $\#D = p$ and suppose that $q|\#G$ for some prime q. The G contains an element of order q and hence a subgroup of order q. Since this subgroup is nontrivial, it has D as a subgroup so that $p|q$ implying that $p = q$. Therefore, G has prime power order. Finally, cince the center of a p–group is nontrivial, we see that D is contained in the center of G.

As an example of this, consider $L = \mathbb{Q}(\zeta_5), K = \mathbb{Q}$. Then $G = \mathbf{C}_4$ and we have a unique subfield $F = \mathbb{Q}(\sqrt{5}) = L^H$ where $H = \mathbf{C}_2$ is in the center of G. Let $p = 19$ (or in fact any prime congruent to $-1 \mod 5$). Since $(5, 19) = 1$, $19 \not| \operatorname{disc}(L)$. We have the factorizations

$$\begin{aligned} x^4 + x^3 + x^2 + x + 1 &\equiv (x^2 + 5x + 1)(x^2 + 15x + 1) \mod 19 \\ x^2 - 5 &\equiv (x - 9)(x + 9) \mod 19, \end{aligned}$$

where all of the factors above are irreducible. We thus have the factorizations

$$\begin{aligned} 19 &= (19, \sqrt{5} - 9)(19, \sqrt{5} + 9) \quad \text{in } \mathbb{Q}(\sqrt{5}), \\ 19 &= (19, \zeta_5^2 + 5\zeta_5 + 1)(19, \zeta_5^2 + 15\zeta_5 + 1) \quad \text{in } \mathbb{Q}(\zeta_5). \end{aligned}$$

Therefore, 19 splits completely in every intermediate field but not in L.

(f) Suppose that P is inert in every intermediate field but not in L. We distinguish two cases. Either P is ramified in L of it splits into at least two distinct primes in L. In the latter case, part c applies and we have that G is cyclic of prime order. In the former case, part d applies and we have that G is of prime power order and contains a unique nontrivial normal subgroup (in fact in the center of G) of prime order. Since L^D is the largest intermediate field in which P splits completely, we see that $L^D = K$ so that $D = G$. We know that D/I is cyclic; therefore G/I is cyclic. But I is in the center of G, and this implies that G is cyclic. Therefore G is cyclic of prime power order.