Math 620, Fall, 1999
Solutions to Take-Home Final Problems

1. In this problem, you may use the facts that in the field $K = \mathbb{Q}(\sqrt{-5})$, the ring of integers is $R = \mathbb{Z}[\sqrt{-5}]$, and (cf. Assignment 5) $C(R)$ is of order 2, with generator the class of the prime ideal $\mathfrak{q} = (3, 2+\sqrt{-5})$. Show that if p is a prime number, then p can be written in the form $p = x^2+5y^2$, with x, $y \in \mathbb{Z}$, if and only if either $p = 5$ or else $p \equiv 1$ or $9 \pmod{20}$.

Solution. First suppose p is a prime number of the form $p = x^2 + 5y^2$, with $x, y \in \mathbb{Z}$. One possibility is clearly that $p = 5$, $x = 0$, $y = \pm 1$. Since $p = 2$ or 3 is impossible (if $y \neq 0$, then $x^2 + 5y^2 \geq 5$, and otherwise $p = x^2$, which is also impossible if p is prime), we may assume p is an odd prime > 5. Reducing $p = x^2 + 5y^2 \bmod 5$, we see $p \equiv x^2 \pmod 5$, so p is a quadratic residue mod 5 and thus $p \equiv \pm 1 \pmod 5$. Reducing $p = x^2 + 5y^2 \bmod 4$, we see $p \equiv x^2 + y^2 \pmod 4$, so p is a sum of two quadratic residues mod 4. Since the quadratic residues mod 4 are 0 and 1, this rules out the possibility that $p \equiv 3 \pmod 4$. So $p \equiv \pm 1 \pmod 5$ and $p \equiv 1 \pmod 4$, which means $p \equiv 1$ or $9 \pmod{20}$.

In the other direction, since we've already disposed of the case $p = 5$, suppose $p \equiv 1$ or 9 (mod 20), i.e., $p \equiv \pm 1 \pmod 5$ and $p \equiv 1 \pmod 4$. The discriminant of R is -20, so p doesn't ramify. Also note that p splits as $\mathfrak{p}\bar{\mathfrak{p}}$ in R, with $\mathfrak{p}$ a prime ideal of R and $\bar{\mathfrak{p}}$ its Galois conjugate, if and only if $x^2 + 5$ has a root mod p, i.e., if and only if -5 is a quadratic residue mod p. Since $p \equiv 1 \pmod 4$ and thus -1 is a quadratic residue mod p, by quadratic reciprocity, this is the same as p being a quadratic residue mod 5, which is the case since $p \equiv \pm 1 \pmod 5$. Now there are two sub-cases. If $\mathfrak{p} = (x+y\sqrt{-5})$, then $p = x^2+5y^2$ and we are done. Otherwise, $\mathfrak{p}$ is non-principal and lies in the ideal class of $\mathfrak{q}$. Then $\mathfrak{p} = c\mathfrak{q}$ with $c \in K^\times$, and thus $p = N_{K/\mathbb{Q}}(\mathfrak{p}) = N_{K/\mathbb{Q}}(c)N_{K/\mathbb{Q}}(\mathfrak{q}) = 3N_{K/\mathbb{Q}}(c)$. Write $c = (a + b\sqrt{-5})/d$, where a, b, $d \in \mathbb{Z}$, $d > 0$, and without loss of generality we may assume a, b, d have no common factor. Then $N_{K/\mathbb{Q}}(c) = (a^2 + 5b^2)/d^2$ and so

$$pd^2 = 3(a^2 + 5b^2).$$

If one of a and d is divisible by 5, then so is the other, and then d^2 and a^2 are both divisible by 5^2 so b is also divisible by 5. This contradicts the assumption that a, b, d have no common factor. So a and d are relatively prime to 5 and a^2, d^2 are each congruent to $\pm 1 \pmod 5$. Thus $\pm p \equiv \pm 3 \pmod 5$, which contradicts the assumption that $p \equiv \pm 1 \pmod 5$. This concludes the proof.

2. Find the fundamental unit for the real quadratic field $K = \mathbb{Q}(\sqrt{10})$, and justify your answer. Also show that the class number of K is 2 by using the Minkowski bound and studying the splitting of small primes. Finally, check that your value of the class number is correct by using the Class Number Formula.

Solution. The ring of integers in K is $R = \mathbb{Z}[\sqrt{10}]$. Write the fundamental unit as $u = x + y\sqrt{10}$ with x, $y \in \mathbb{Z}$, $u > 1$, $x^2 - 10y^2 = (x + y\sqrt{10})(x - y\sqrt{10}) = \pm 1$. x can't be negative, since then either u or its Galois conjugate ($= u^{-1}$) has both terms negative, so $u < 0$. So the fundamental unit comes from the solution of $x^2 - 10y^2 = \pm 1$ with $x \geq 0$ minimal. Clearly $x = 0$, 1, 2 don't work, so the fundamental unit is $u = 3 + \sqrt{10}$ with norm -1.

The discriminant of R is $4 \cdot 10 = 40$. So by Minkowski, every element of $C(R)$ has a representative with norm bounded by

$$\frac{2!}{2^2}\sqrt{40} = \sqrt{10} = 3.16\cdots .$$

So we only have to look at the splitting of the primes 2 and 3. Let $\mathfrak{p} = (2, \sqrt{10})$ and $\mathfrak{q} = (3, 1+\sqrt{10})$. Clearly $\mathfrak{p}$ strictly contains (2) and $\mathfrak{q}$ strictly contains (3). Now each element of $\mathfrak{p}$ is of the form

$x + y\sqrt{10}$ with x, $y \in \mathbb{Z}$, x even, and thus has norm $x^2 - 10y^2 \equiv 0 \pmod 2$. So $\mathfrak{p}$ is a proper ideal of R containing (2) and must therefore be the prime ideal with $(2) = \mathfrak{p}^2$. (Recall 2 has to ramify.) Similarly, every element of $\mathfrak{q}$ is of the form

$$3(a + b\sqrt{10}) + (1 + \sqrt{10})(c + d\sqrt{10}) = (3a + c + 10d) + (3b + c + d), \quad a, b, c, d \in \mathbb{Z},$$

with norm $(3a+c+10d)^2 - 10(3b+c+d)^2 \equiv (c+d)^2 - (c+d)^2 \equiv 0 \pmod 3$, so $\mathfrak{p}$ is a proper ideal of R containing (3) and must therefore be a prime ideal with $(3) = \mathfrak{q}\bar{\mathfrak{q}}$ ($\bar{\mathfrak{q}}$ the Galois conjugate). Now $\mathfrak{p}$ can't be principal, since there is no element of R of norm ± 3. (If $x^2 - 10y^2 = \pm 3$, then reducing mod 5, $x^2 \equiv \pm 3 \pmod 5$, which is impossible.) Since $\mathfrak{p}^2 = (2)$, $\mathfrak{p}$ therefore represents an element of $C(R)$ of order 2. But $\mathfrak{pq} = (6,\ 3\sqrt{10},\ 2 + 2\sqrt{10},\ 10 + \sqrt{10})$ has norm $2 \cdot 3 = 6$ and contains $2 + \sqrt{10} = 2 + 2\sqrt{10} - 3\sqrt{10}$, which has norm $2^2 - 10 = -6$, so $\mathfrak{pq} = (2 + \sqrt{10})$ is principal and thus $\mathfrak{p}$, $\mathfrak{q}$, $\bar{\mathfrak{q}}$ all represent the same element of $C(R)$. Hence $C(R)$ is of order 2.

We can confirm this using the class number formula

$$h_K = \frac{(2)\sqrt{40}}{4\,\mathrm{reg}(K)} L(1,\ \chi) = \frac{\sqrt{10}}{\log u} L(1,\ \chi),$$

where χ is the multiplicative character defined by splitting in K. This works out to (see Janusz, Theorem VI.4.5)

$$\begin{aligned} \frac{1}{\log(3 + \sqrt{10})} \Bigg| & \chi(1) \log \sin\left(\frac{\pi}{40}\right) + \chi(3) \log \sin\left(\frac{3\pi}{40}\right) + \chi(7) \log \sin\left(\frac{7\pi}{40}\right) \\ & + \chi(9) \log \sin\left(\frac{9\pi}{40}\right) + \chi(11) \log \sin\left(\frac{11\pi}{40}\right) + \chi(13) \log \sin\left(\frac{13\pi}{40}\right) \\ & + \chi(17) \log \sin\left(\frac{17\pi}{40}\right) + \chi(19) \log \sin\left(\frac{19\pi}{40}\right) \Bigg|, \end{aligned}$$

where we find that $\chi = 1$ at 1, 3, 9, 13 and $\chi = -1$ at 7, 11, 17, 19 (since 10 is a quadratic residue mod 3 or 13 but not mod 7, mod 11, mod 17, or mod 19). The formula works out to 2 (amazingly enough!): the sum inside the absolute value signs is -3.63689, and $\log u = 1.81845$.

3. Let $K = \mathbb{Q}(\sqrt{-3})$, which contains a primitive cube root of unity, $\omega = (-1 + \sqrt{-3})/2$. You may use the fact that the ring of integers $R = \mathbb{Z}[\omega]$ of K is a Euclidean ring, hence a PID. First classify the non-zero prime ideals $\mathfrak{p}$ of R, or equivalently the irreducible elements of R up to multiplication by 6th roots of unity, (according to the prime numbers $p \in \mathbb{Z}$ that they sit over) by studying the splitting of prime numbers p in R.

Solution. The discriminant of R is -3, so 3 is the only prime that ramifies, and $\sqrt{-3}$ is irreducible sitting over 3 (and unique up to 6th roots of unity with this property). Since $R = \mathbb{Z}[\omega]$ and the minimal polynomial of ω is $x^2 + x + 1$, which is irreducible mod 2, the prime 2 is inert in R, and 2 remains irreducible. For primes $p > 3$, p splits in R if and only if $x^2 + 3$ has a root mod p, or $\left(\frac{-3}{p}\right) = 1$. But

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1, & p \equiv 1 \pmod 3, \\ -1, & p \equiv 2 \pmod 3. \end{cases}$$

So primes $p \equiv 2 \pmod 3$ remain irreducible in R and primes $p \equiv 1 \pmod 3$ split as products of two distinct irreducibles (not associates, but complex conjugates of one another).

Problem (continued). Next, consider the extension field $L = K(\sqrt[3]{5})$ of K. Show that L is a cyclic Galois extension of K with Galois group G generated by $\sigma\colon \sqrt[3]{5} \mapsto \omega\sqrt[3]{5}$. Compute the Artin map $\varphi_{L/K}$ for L over K, in the sense of computing $\varphi_{L/K}(\mathfrak{p}) \in G$ for all but finitely many non-zero prime ideals $\mathfrak{p}$ of R.

Solution. L is generated over $\mathbb{Q}$ by $\sqrt[3]{5}$ and by ω, so it is the splitting field of $x^3 - 5$, which has roots $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$, and $\omega^2\sqrt[3]{5}$. Thus L is Galois over $\mathbb{Q}$ and over K, and since $x^3 - 5$ is irreducible over K, L has degree 3 over K with cyclic Galois group generated by σ.

The discriminant of the minimal polynomial of $x^3 - 5$ is $-3^3 \cdot 5^2$, and since the discriminant of R is -3, the primes of $\mathbb{Z}$ that ramify in L must be 3 and 5. (The prime 3 already ramifies in K, and $5 = \left(\sqrt[3]{5}\right)^3$.) It turns out that no primes of $\mathbb{Z}$ can remain inert in L, since otherwise we would have an injection of $\mathrm{Gal}\,(L/\mathbb{Q}) = S_3$ into a cyclic group, which is impossible. So over a prime number p in $\mathbb{Z}$ other than 3 or 5, we can have 2, 3, or 6 primes of L. (All of these cases occur.) If $p \equiv 2 \pmod 3$, then $(p-1,\, 3) = 1$, so every element of $\mathbb{F}_p^\times$ has a cube root. Thus 5 has a cube root mod p, so p must split at least partially in $\mathbb{Q}(\sqrt[3]{5})$ and must split into exactly 3 primes in L (since p does not split in K). Thus $\varphi_{L/K}(p) = 1$.

Therefore suppose $p \equiv 1 \pmod 3$. In this case there are two primes $\mathfrak{p}$ over p in K. Since $p-1$ is divisible by 3, exactly one third of the elements of $\mathbb{F}_p^\times$ have a cube root. So 5 may or may not have a cube root mod p, depending on the value of $5^{(p-1)/3}$ in $\mathbb{F}_p^\times$. This value must be a cube root of 1. If it is 1, 5 has a cube root mod p and thus p must split at least partially in $\mathbb{Q}(\sqrt[3]{5})$. So 3 must divide the number of primes over p in L, and each $\mathfrak{p}$ over p in K splits further into three prime factors in L. Then again $\varphi_{L/K}(p) = 1$.

Finally, if $p \equiv 1 \pmod 3$ and $5^{(p-1)/3} \not\equiv 1 \pmod p$, then 5 does not have a cube root mod p and the two primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ over p in K remain inert in L. So in this case, $\varphi_{L/K}(\mathfrak{p}) = \sigma$ or σ^2, where σ is the generator of G as in the statement of the problem. Note that $\mathfrak{p}$ has norm p, so $R/\mathfrak{p} \cong \mathbb{F}_p$ and the Frobenius generator of $\mathrm{Gal}\left((R'/R'\mathfrak{p})/(R/\mathfrak{p})\right)$, where R' is the ring of integers in L, is given by raising to the p-th power. We have to see if it matches up with σ or σ^2. This is simply an issue of the value of $5^{(p-1)/3} \bmod p$. If this corresponds to ω (i.e., is the image of ω under the map $R \to R/\mathfrak{p} \cong \mathbb{F}_p$), that means $\left(5^{1/3}\right)^{p-1}$ corresponds to ω, or $\left(5^{1/3}\right)^p$ corresponds to $\omega\, 5^{1/3}$, which means the Frobenius element matches up with σ; otherwise, it matches up with σ^2. Note incidentally that $\varphi_{L/K}(\mathfrak{p})$ and $\varphi_{L/K}(\bar{\mathfrak{p}})$ are inverses of each other, since the images of ω under the maps $R \to R/\mathfrak{p} \cong \mathbb{F}_p$ and $R \to R/\bar{\mathfrak{p}} \cong \mathbb{F}_p$ have to be different. (Otherwise, since R is generated over $\mathbb{Z}$ by ω, the maps themselves would be the same and $\mathfrak{p}$ would coincide with $\bar{\mathfrak{p}}$, which is not the case.)