FINAL EXAM SOLUTIONS: MAT 415

Solution to Problem 1a:

$(x, y) = (-1, 2)$ gives 7, and so henceforth assume $p \neq 7$. Then working modulo 7, we see that $x^2+xy+2y^2 \equiv (x-3y)^2$, and thus any p representable in such a way must be a quadratic residue mod 7, and hence either $1, 2$ or 4. Thus we only need prove sufficiency. So assume that p is a quadratic residue mod 7.

Consider the field $K = \mathbb{Q}(\sqrt{-7})$. Then since $-7 \equiv 1 \mod 4$ we learn that $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot \frac{-1+\sqrt{-7}}{2}$. Noting $Nm_{K/\mathbb{Q}}(x + y \cdot \frac{1+\sqrt{-7}}{2}) = x^2 + xy + 2y^2$, we see that we must determine which primes p can be written as $\mathrm{Nm_{K/Q}}(\alpha)$ for $\alpha \in \mathcal{O}_K$. Now, the Minkowski bound immediately tells us that the class number of K is 1, and hence every ideal is principal.

By quadratic reciprocity, since p is a quadratic residue mod -7, we learn that -7 is a quadratic residue mod p, and hence p splits in K as $(p) = P_1P_2$ for prime ideals P_1, P_2 of norm p. Since K is a PID, let $P_1 = (\alpha)$. Then $(\mathrm{Nm_{K/\mathbb{Q}}}\alpha) = (\mathrm{p})$ and hence $\mathrm{Nm}(\alpha) = \pm \mathrm{p}$, and since all norms from K are positive, we get the result.

Solution to Problem 1b:

As in the previous problem, this problem asks for primes which are norms of elements from $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-5})$. The Minkowski bound here is

$$\sqrt{20} \cdot \frac{2!}{2^2} \cdot \frac{4}{\pi} < \frac{\sqrt{80}}{3} < 3.$$

Now $2\mathcal{O}_K$ factors as I_2^2, where $I_2 = (2, 1 + \sqrt{-5})$. Moreover, I_2 is not principal, as 2 cannot be a written as $x^2 + 5y^2$. Thus, the class group of K is $\mathbb{Z}/2\mathbb{Z}$ generated by $[I_2]$.

Now, if p is an odd prime that doesn't equal 5, but can be written as $x^2 + 5y^2$, a congruence check shows that it must be 1 modulo 4, and 1 or 4 mod 5, and thus either 1 or 9 mod 20.

Conversely, suppose p is either 1 or 9 mod 20. Then since p is a quadratic residue mod 5, it means that 5 is a quadratic residue mod p by quadratic reciprocity. Since p is relatively prime to 20, it follows that p is unramified in K. Thus, (p) splits as $(p) = P_1P_2$. It remains to show that P_1 is principal. Assume it is not for the sake of contradiction. Then P_1I_2 is principal, and thus equals $\alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K$. Thus $\mathrm{Nm_{K/\mathbb{Q}}}(\alpha) = 2\mathrm{p}$. However, $2p$ is not a quadratic residue modulo 5, so this is a contradiction. Thus, P_1 is

principal, and this completes the proof.

Solution to Problem 2

We first claim that the class group of K is trivial. Indeed, the Minkowski bound is $\frac{\sqrt{21}}{2} < 3$. Moreover, $2\mathcal{O}_K$ is a prime ideal, and is thus principal. Thus, the class group of K is indeed principal.

Assume that L is a quadratic extension of K which is unramified. Since K contains the second roots of unity, we can write $L = K(\sqrt{d})$, where we may multiply d by any square in K. Since $d\mathcal{O}_L$ is a square in L, and L is unramified over K, it follows that $d\mathcal{O}_K$ is a square in K as well. Indeed, if $d\mathcal{O}_L = \prod_i Q_i^{2m_i}$ or prime ideals Q_i of $\mathcal{O}_L$, then by unique factorization one can verify that we must have $d\mathcal{O}_L = \prod_i P_i^{2m_i}$ where P_i is the unique prime ideal of $\mathcal{O}_K$ lying under Q_i.

Now, since $\mathcal{O}_K$ is a PID, we can write $d\mathcal{O}_K = \alpha^2\mathcal{O}_K$, and as $L = K(\sqrt{d/\alpha^2})$ we may as well replace d by d/α^2 and thus assume that $d \in \mathcal{O}_K^\times$.

Next, note that $\mathcal{O}_K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and thus $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$. Thus there are only 3 candidate fields L to check. It is straightforward to verify that $\beta = \frac{5-\sqrt{21}}{2}$ is a fundamental unit, and thus the 3 candidate fields are

$$K(\sqrt{\beta}), K(\sqrt{-\beta}), K(\sqrt{-1}).$$

As $3\beta = \left(\frac{3-\sqrt{21}}{2}\right)^2$, the 3 candidate fields can be rewritten as

$$K(\sqrt{3}), K(\sqrt{-1}), K(\sqrt{-3})$$

.

Next, note that the first two fields contain $\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-i})$ resp., whose discriminants are divisible by 2. Thus the prime 2 ramifies in these fields, but it does not ramify in K. It follows that the primes about 2 in K must ramify in $K(\sqrt{-3})$ and $K(\sqrt{-1})$.

As for $L = K(\sqrt{-3})$, we claim that this field is unramified over K. By the Dedekind-Kummer theorem, as $x^2 - 3$ is separable modulo all primes distinct from $2, 3$ it follows that the only primes of K ramified in L must lie above 2 or 3. But similarly, we can write $L = K(\sqrt{-7})$, and applying the same argument to the polynomial $x^2 - 7$ shows that only the primes of K that lie above 2 may ramify in L. Thus we will be done if we can show that 2 does not ramify in L.

To see this, note first that as $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$ it is Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}/2\mathbb{Z}$. Now let Q be any prime of L above 2, and let I_Q be the inertia group of Q. Then if I_Q is non-trivial, we may find a $\mathbb{Z}/2\mathbb{Z}$ quotient of the Galois group such that the image of I_Q in this quotient remains non-trivial. Hence, 2 must ramify in at least one of the 3 quadratic fields contained in L. But these are $\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{21})$, and since 2 does not ramify in all of them this is a contradiction. Hence 2 is unramified in

L, and the proof is complete.

Solution to Problem 3a

Note first that K cannot contain any roots of unity besides ± 1, since K is Galois of odd degree and thus must be totally real. Let $P_1, \ldots, P_r$ be the ramified primes of K over $\mathbb{Q}$, and $p_1, \ldots, p_r$ the rational primes under them, so that $p_i \mathcal{O}_K = P_i^3$. Let the Galois group of K over $\mathbb{Q}$ be written as $G = \{1, \sigma, \sigma^2\}$. An important observation is that the ideals P_i are fixed by the group G.

Now, consider the homomorphism $\phi : (\mathbb{Z}/3\mathbb{Z})^r \to Cl(K)[3]$ given by

$$(a_1, \ldots, a_r) \to [\prod_i P_i^{a_i}].$$

We claim that the kernel of ϕ is at most of size 3, which will solve the problem, as it implies that size of the image of ϕ is at least 3^{r-1}.

To see this, let $\vec{a} \in \ker \phi$ so that $I := \prod_i P_i^{a_i}$ is principal. Say $I = (x)$. Then as $I = \sigma(I)$ we have that $x/\sigma(x) \in \mathcal{O}_K^\times$.

Lemma 0.1. *Consider the map $h : \mathcal{O}_K^\times / \pm 1 \to \mathcal{O}_K^\times / \pm 1$ given by $h(u) = u/\sigma(u)$. Then the image of h has index of size 3.*

Proof. Consider the logarithmic embedding $\log_K : K^\times \to \oplus_{g \in G} (\mathbb{R}^\times)_g$ given by the archemedian embeddings of K. We know from Dirichlet's unit theorem that $\log_K(\mathcal{O}_K^\times)$ is a lattice of rank 2, contained in the hyperplane of product 1. Moreover, the linear map $1 - \sigma$ acts on this hyperplane with eigenvalues $1 - \omega, 1 - \omega^2$ where ω is a primitive 3rd root of unity. Thus the determinant of $1 - \sigma$ acting on this hyperplane is $(1 - \omega)(1 - \omega^2) = 3$.

Moreover, $\log_K(h(u)) = (1 - \sigma) \log_K(u)$, and $\log_K$ is an isomorphism on $\mathcal{O}_K^\times / \pm 1$ since it only kills the roots of unity. The result follows. □

Now, for $I \in \ker \phi$, we define $f(I) \in \operatorname{coker}(h)$ to be the image of $x/\sigma(x)$ in $\operatorname{coker}(h)$. This is well defined as multiplying x by a unit $u \in \mathcal{O}_K^\times$ multiplies the value of $x/\sigma(x)$ by $u/\sigma(u)$, and thus doesn't change the image in $\operatorname{coker}(h)$. We thus get a homomorphism $f : \ker \phi \to \operatorname{coker}(h)$. We claim that f is injective. To see this, suppose that $f(\vec{a})$ is trivial. It means that we can write $I = \prod_i P_i^{a_i}$ as (x) such that $x/\sigma(x)$ maps to 1 in $\operatorname{coker}(h)$. Thus, by replacing x by xu for some unit u, we can assume that $x/\sigma(x) \in \pm 1$. Finally, replacing I by I^2 we can assume that $x/\sigma(x) = 1$. This means that $x = \sigma(x)$ and thus that $x \in \mathbb{Q}$. However, the ideal $\prod_i P_i^{a_i}$ only comes from an ideal in $\mathbb{Q}$ if all the a_i are divisible by 3. Thus, f is injective, and thus the size of $\ker \phi$ is at most 3, which completes the proof.

Solution to Problem 3b.

We continue using notation from above.

Note first that the group G acts on $M = Cl(K)[3]$ in the obvious way. Now, consider that map $\psi : Cl(K)[3] \to Cl(K)[3]^G$ given by $\psi([I]) = [I/\sigma(I)]$. Clearly ψ is an endomorphism of $Cl(K)[3]$. To see that the image of ψ lands in the invariant part of $Cl(K)[3]$ by G, it is enough to show that $[I/\sigma(I)] = [\sigma(I)/\sigma^2(I)]$, or in other words that $[I\sigma(I)\sigma^2(I)] = [\sigma(I^3)]$. However, the LHS is trivial since the norm of any ideal is a rational ideal and thus principal, and the RHS is trivial since I was assumed to be of order 3 in the class group. Thus, ψ is a homomorphism. Clearly, the kernel of ψ is $Cl(K)[3]^G$, and thus we have proven that

$$|Cl(K)[3]| \leq |Cl(K)[3]^G|^2.$$

It thus suffices to bound $|Cl(K)[3]^G|$ by 3^r. To do this, suppose $[I] = [\sigma(I)]$ for some 3-torsion ideal class $[I]$. Then we can write $I = x\sigma(I)$, and thus taking norms we see that $\mathrm{Nm_{K/\mathbb{Q}}x} \in \mathbb{Q} \cap \mathcal{O}_\mathrm{K}^\times = \pm 1$. By replacing x by $-x$, we can assume that $\mathrm{Nm_{K\mathbb{Q}}x} = 1$. Thus, by Hilberts theorem 90, we can write $x = \sigma(y)/y$ for some $y \in K^\times$. It follows that $Iy = \sigma(Iy)$. Now, expanding Iy as a product of powers of prime ideals, it follows that one may write Iy as the product of powers of the P_i and rational primes. Thus, we see that $[I]$ is contained in the image of the map ϕ we have defined earlier. This image is clearly of size at most 3^r, which completes the proof.

Solution to Problem 3c.

We may proceed exactly as above, only now we need to show that the image of ϕ is of size at most 3^{r-1} (and thus exactly 3^{r-1} by the argument in part a).

To see this, pick an element $u \in \mathcal{O}_K^\times$ such that neither u nor $-u$ is representable as $y\sigma(y)$ for $y \in \mathcal{O}_K^\times$ (such a u exists by the lemma in part a). Now, wlog u has norm 1 and $-u$ has norm -1. Thus, by Hilberts theorem 90 we may write $u = y/\sigma(y)$ for $y \in K^\times$.

Moreover, since $(y) = (\sigma(y))$ we may write (y) as the product of powers of the P_i and rational primes, thus we may write $(y) = \prod_i P_i^{a_i} \cdot q$ for some rational number q. Now, if all the a_i were divisible by 3, then we could write $y = v \cdot q \prod_i p_i^{a_i/3}$ for some $v \in \mathcal{O}_K^\times$, and thus

$$u = y/\sigma(y) = v/\sigma(v)$$

which is a contradiction. Thus the a_i are not all divisible by 3, and so $\vec{a}$ represents a non-trivial element of the kernel of ϕ, as desired.

Solution to Problem 4a.

Assume p, q are both odd for now. Then pick a natural number a relatively prime to q such that aq is a quadratic residue modulo p. Then by Hensel's lemma, aq is a square in $\mathbb{Q}_p$, while aq cannot be a square in $\mathbb{Q}_q$ as it has odd valuation ($v_q(aq) = 1$). Thus the fields are not isomorphic.

Now, assume that $p = 2$ and q is odd. Then as we have shown in class, $\mathbb{Q}_2$ has 7 quadratic extensions while $\mathbb{Q}_p$ has only 3. Thus the fields are not isomorphic.

Solution to Problem 4b.

First note that any automorphism of $\mathbb{Q}_p$ must preserve 1, and hence must preserve $\mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, it suffices to show that any such automorphism is continuous.

Let $S = \{x \in \mathbb{Q}_p \mid 1 + p^3x^4 \text{ is a square}\}$. It is easy to see that $S = \mathbb{Z}_p$, since if $x \notin \mathbb{Z}_p$ then $v_p(1 + p^3x^4) = v_p(p^3x^4) = 4v_p(x) + 3$ is odd, and if $x \in \mathbb{Z}_p$ one may use Hensel's lemma (the stronger version in the case $p = 2$). Thus any automorphism must preserve $\mathbb{Z}_p$, and hence $p^m\mathbb{Z}_p$ for any integer m. Hence valuations are preserved, and thus the automorphism is continuous.

Solution to problem 5

Assume such an L exists for the sake of contradiction. Let $G = S_3$ be the Galois group of $L/\mathbb{Q}_7$, and let G_i be the higher ramification groups. Then as G_i/G_{i+1} are 7-groups for $i > 1$, we conclude that G_2 is trivial. Moreover, G_1 is normal in $G_0 = G$ and thus G_1 is either trivial, S_3 or A_3. Since G_0/G_1 and G_1/G_2 are always cyclic, we conclude that $G_1 = A_3$. Thus, the unique quadratic subfield F of L is unramified over $\mathbb{Q}_7$, and thus is the unique unramified extension of $\mathbb{Q}_7$. Moreover, L is cyclic over F of degree 3. Since F (and in fact $\mathbb{Q}_7$) contain the 3rd roots of unity, we can write $L = F(\sqrt[3]{d})$ for some $d \in F^\times$. Now,

$$F^\times = 7^{\mathbb{Z}} \oplus \mu_{48} \oplus (1 + 7\mathcal{O}_F),$$

where μ_{48} are the 48'th roots of unity. Thus, we see that $F^\times/(F^\times)^3 \cong 7^{\mathbb{Z}/3\mathbb{Z}} \oplus \mu_3$. It follows that we may take $d \in \mathbb{Q}_7^\times$, and thus $\mathbb{Q}_7(\sqrt[3]{d})$ is a cyclic cubic extension of $\mathbb{Q}_7$ contained in L. However, this contradicts Galois theory since S_3 has no normal subgroups of index 3.