

Math 248b, Winter 2003
Problem Set 1, Friday, January 30, 2004

- (1) Work out the Artin symbols for quadratic number fields. That is, begin with $\mathbb{Q}(\sqrt{q})$ where q is an odd prime and identify the Galois group with $\{\pm 1\}$. Check that the Artin symbol σ_p is exactly the Legendre symbol (q/p) under this identification. Now try the same for more complicated quadratic fields and for the cyclotomic field $\mathbb{Q}(\zeta_m)$.

- (2) The “inclusion theorem” is the key step in showing one direction of the Abelian Polynomial theorem. That is, if $Spl(f)$ can be defined by congruence conditions, then $f(x)$ must be an abelian polynomial. The inclusion theorem states:

Theorem 1. *Suppose $f(x)$ and $g(x)$ are polynomials with splitting fields K_f and K_g respectively. Then $K_f \subseteq K_g$ if and only if $Spl(g) \subseteq Spl(f)$ for almost all primes.*

Show that $K_f \subseteq K_g$ implies $Spl(g) \subseteq Spl(f)$ for almost all primes. (The other direction follows from Chebotarev density.) Explain why this result proves the piece of the Abelian polynomial theorem (via cyclotomic fields) and then show how this same proof together with Artin reciprocity, implies Kronecker’s theorem.

Theorem 2 (Kronecker). *Every abelian extension of \mathbb{Q} is contained in a cyclotomic extension.*

- (3) Use the Chebotarev Density Theorem to show the Artin map is surjective.
- (4) Show that for any fixed k ,

$$\sum_{\zeta^n=1} \zeta^k = \begin{cases} n & \text{if } n|k \\ 0 & \text{otherwise} \end{cases}$$

- (5) One key in Dirichlet’s theorem on primes in arithmetic progressions was the evaluation of Gauss sums, which allowed $L_{-1}(1)$ to be expressed as a finite sum of characters. Now define a generalized Gauss sum

$$G(m, d) = \sum_{r(\bmod d)} \left(\frac{r}{d}\right) e\left(\frac{mr}{d}\right)$$

where the character may be appropriately defined as an n th power residue symbol in a number field containing the n th roots of unity. For simplicity, suppose the character is quadratic, or cubic with $d \equiv 1(3)$, i.e. $n = 2$ or 3 . Prove the following properties of the Gauss sum:

- (a) If d and d' are coprime, then

$$g(m, dd') = \left(\frac{d}{d'}\right) \left(\frac{d'}{d}\right) g(m, d)g(m, d')$$

(b) If k and d are coprime, then

$$g(mk, d) = \left(\frac{k}{d}\right)^{-1} g(m, d)$$

(c)

$$g(p^k, p^l) = \begin{cases} p^k g_l(1, p) & \text{if } l = k + 1; \\ \phi(p^l) & \text{if } n|l, k \geq l; \\ 0 & \text{otherwise} \end{cases}$$

$$\text{where } g_l(m, d) = \sum_{r \pmod{d}} \left(\frac{r}{d}\right)^l e\left(\frac{mr}{d}\right)$$

(6) Prove the following result (sketched in class):

Proposition 1. *Let $D \equiv 0, 1(4)$ be an integer and m an odd integer relatively prime to D . Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue modulo m .*

Conclude that for $(n, p) = 1$, then $\left(\frac{-n}{p}\right) = 1$ if and only if p is represented by a primitive form of discriminant $-4n$.

(7) Show that every primitive positive definite form is properly equivalent to a unique reduced form, that is, a form $f(x, y) = ax^2 + bxy + cy^2$ such that $|b| \leq a \leq c$ and $b \geq 0$ if $|b| = a$ or $a = c$.

HINT: First show that any form is equivalent to one satisfying $|b| \leq a \leq c$. The idea is that, given any form, we can pick a form in the equivalence class with $|b|$ minimal. Then use elements of $SL(2, \mathbb{Z})$ (in this case, translations) to get the result. Now we just need to show that it is reduced. So we're done unless both $b < 0$ and $a = -b$ or $a = c$. This amounts to showing that $ax^2 \pm bxy + cy^2$ are properly equivalent. Again, you just need the right automorphism from $SL(2)$. Last, the hard part: we need to show uniqueness. The proof is due to Legendre and relies on finding the smallest numbers properly represented by a form satisfying $|b| \leq a \leq c$. Then showing that these values determine the a, b and c coefficients for these representative forms. You need to find the smallest three numbers represented to have enough conditions to solve for a, b, c . First show

$$f(x, y) \geq (a - |b| + c) \min(x^2, y^2)$$

and you're off...

This implies that the three smallest values represented by $f(x, y)$ are $a < c < a - |b| + c$. Now suppose that $g(x, y)$ is any other form for which these three values are the smallest represented. One shows that the first and last coefficients of g must be a and c . According to the discriminant, g must be $ax^2 \pm bxy + cy^2$. If the forms f and g are properly equivalent, then we have restrictions on the form of the element of $PSL(2, \mathbb{Z})$ which shows that $f = g$, completing the proof.

Use this result to conclude that for $D < 0$, then $h(D)$, the number of classes of primitive positive definite quadratic forms of discriminant D , is finite.

Can you use this fact, together with the connection between quadratic forms and quadratic fields discussed in class, to conclude that imaginary quadratic fields have a finite class group? Why or why not? Also, make the connection between automorphisms of quadratic forms and the number of units in imaginary quadratic fields in order to justify the values ω used in the proof of Dirichlet's class number formula.

- (8) Prove the following identity involving an important integral transform for any positive integer k , and real numbers $c, y > 0$:

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{y^s ds}{s(s+1)\cdots(s+k)} = \begin{cases} 0 & \text{if } y \leq 1 \\ \frac{1}{k!} \left(1 - \frac{1}{y}\right)^k & \text{if } y \geq 1. \end{cases}$$