Solutions
Algebra Midterm
Math 123 – Harvard University – Spring 2002

1. Factor $1+5i$ into primes in the Gaussian integers $\mathbb{Z}[i]$.

   Answer: $(1+5i) = (1+i)(3+2i)$. To arrive at this answer, note that $N(1+5i) = 26 = 2\cdot 13$. Since $2 = (1+i)(1-i)$ and $\mathbb{Z}[i]$ is a UFD, we know either $1+i$ or $1-i$ divides $1+5i$. Trying $1+i$ we obtain the factorization above. Since $N(1+i) = 2$ and $N(3+2i) = 13$ are primes in $\mathbb{Z}$, the factors $1+i$ and $3+2i$ are primes in $\mathbb{Z}[i]$.

2. Find the ideal class group of $\mathbb{Z}[\sqrt{-13}]$. Justify your answer. (Hint: $4\sqrt{13} < 15$).

   Answer: Since $-13 = 3 \bmod 4$, the ring $R = \mathbb{Z}[\sqrt{-13}]$ is the full ring of integers in $\mathbb{Q}(\sqrt{-13})$. Thus $\Delta(R) = \sqrt{13}$ and $\mu = 4\sqrt{13}/\pi < 15/\pi < 5$. So the class group is generated by the prime divisors of 2 and 3 in R.

   The equation $x^2 = -13 = 2 \bmod 3$ has no solutions, so 3 is inert and does not contribute to the class group. On the other hand, $x^2 = -13 = 1 \bmod 2$ has a solution, so the principal ideal (2) factors as $P\overline{P}$ with $N(P) = 2$.

   Now let I be the lattice generated by (2) and $x = 1 + \sqrt{-13}$. Since

   $$\sqrt{-13}\cdot x = \sqrt{-13} - 13 = 2\cdot(-7) + (1+\sqrt{-13})$$

   belongs to I, we see I is an ideal properly extending (2). Thus $I|(2)$ and therefore we can take $I = P$. Then it is clear that $P = \overline{P}$; that is, $P^2 = (2)$. Moreover P is not principal, since $N(P) = 2$ while $N((a+b\sqrt{-13})) = a^2 + 13b^2$ is never 2. Since P generates the ideal class group, we have $\mathcal{C} \cong \mathbb{Z}/2$.

3. Let $f, g \in \mathbb{Q}[x]$ be irreducible polynomials with a common zero in $\mathbb{C}$. Prove $(f) = (g)$.

   Answer: Since $\mathbb{Q}[x]$ is a PID and f, g are irreducible, the ideals (f) and (g) are maximal. So if $(f) \neq (g)$ then $(f, g) = \mathbb{Q}[x]$. That means we can find a, b such that $af + bg = a(x)f(x) + b(x)g(x) = 1$. Evaluating both sides at any point $z \in \mathbb{C}$, we see $f(z)$ and $g(z)$ cannot both be equal to zero. $\mathbb{Q}[x]$ is

4. Is the polynomial $f(x) = 1 - x + x^2 - x^3 + x^4 - x^5 + x^6$ irreducible in $\mathbb{Z}[x]$? Justify your answer. (Hint: $f(x)$ is part of a geometric series.)

   Answer: This polynomial is irreducible. Indeed,

   $$f(-x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = (x^7 - 1)/(x - 1)$$

   is just the cyclotomic polynomial for the 7th roots of unity. As shown in Artin using Eisenstein's criterion, this polynomial is irreducible. Therefore $f(x)$ is irreducible. (If $f(x) = g(x)h(x)$ then $f(-x) = g(-x)h(-x)$.)