MATH 4108
FINAL EXAMINATION

Name	

1	2	3	4	5	Total

- There are 5 problems on this exam. Please solve **at least 4** of them. If you solve all 5, I'll count the highest 4 scores toward your grade.
- Each problem is worth 20 points, for a maximum score of 80. There are five points of extra credit available on Problem 4.
- The exam is due on **Thursday, April 30, before 5pm**. You can either email me your solutions, or slip them under my office door.
- You may use your course notes and completed homework assignments, the textbook, and a graphing calculator. No other aids are permitted, and you are **not** allowed to discuss the problems with your classmates.
- All answers must be justified unless otherwise noted, and all proofs must be written in clear and grammatical English.
- You may cite any theorem, lemma, proposition, etc. proved in class or in the sections we covered in the text, in addition to any assigned homework problem.
- Good luck, and **start early**!

Problem 1.

Prove that the roots of the polynomial $x^5 - 4x - 1 \in \mathbf{Q}[x]$ are not solvable by radicals.

Solution.

This polynomial is irreducible modulo 3, so it is irreducible over $\mathbf{Q}$. It has exactly three real roots, so its Galois group is S_5 by Corollary 16.12.6. Therefore its roots are not solvable by Theorem 16.12.4.

Problem 2.

Let $d < 0$ be a squarefree integer which is congruent to 1 modulo 4. Let $\delta = \sqrt{d}$, $\eta = \frac{1}{2}(1+\delta)$, and $h = \frac{1}{4}(1-d)$, and let

$$f(x) = (x-\eta)(x-\overline{\eta}) = x^2 - x + h,$$

the minimal polynomial for η. Let $R = \mathbf{Z}[\eta]$, and *suppose that R is a unique factorization domain*. Thus we know from Heegner's theorem that $d \in \{-3,-7,-11,-19,-43,-67,-163\}$, but you may not use this fact as we haven't proven it.

i. Prove that $N(\eta) = h$ and that η has minimal norm among all elements of $R \setminus \mathbf{Z}$. [Draw a picture.]

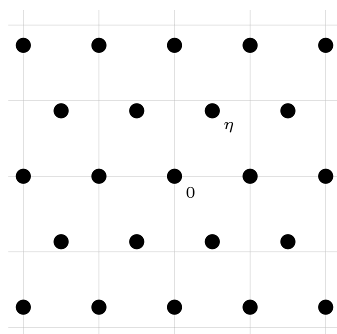
ii. Prove that every prime integer $p < h$ is prime in R.

iii. Let m be a positive integer with $m < h$. Prove that $f(m)$ is a prime integer. [Hint: first show $f(m) < h^2$.]

In particular, taking $d = -163$, the minimal polynomial is $f(x) = x^2 - x + 41$, and the forty values $f(1), f(2), f(3), \ldots, f(40)$ are all prime numbers!

Solution.

i. We have $N(\eta) = \eta\overline{\eta} = f(0) = h$. It is clear from the picture that if $\alpha = a + b\eta$ then $|\alpha| > |\eta|$ if $|b| \geq 2$ or if $|b| = 1$ and $\alpha \notin \{\pm\eta, \pm(\eta-1)\}$.



ii. Suppose $p < h$ is not prime in R. Then $(p) = P\overline{P}$ for a prime ideal P. Since P is principal, $P = (\alpha)$ for some $\alpha \in R$. Clearly $\alpha \notin \mathbf{Z}$ since p is a prime integer. But $N(\alpha) = p < h$, which is impossible by (i).

iii. First note that if $0 < m < h$ then

$$f(m) = m^2 - m + h = m(m-1) + h < h(h-1) + h = h^2.$$

If $f(m)$ is not prime then its smallest prime divisor p is at most $\sqrt{f(m)} < h$. By (ii), we know that p is prime in R. Since

$$p \mid f(m) = (m-\eta)(m-\overline{\eta})$$

we have $p \mid m \pm \eta$, which is impossible since $\eta/p \notin R$.

Problem 3.

Let $\delta = \sqrt{-17}$ and let $R = \mathbf{Z}[\delta]$, the quadratic integer ring in $\mathbf{Q}(\delta)$. Calculate the class group of $\mathbf{Q}(\delta)$, and give representatives for all of the ideal classes.

Solution.

We know from Theorem 13.7.10 that $\mathrm{Cl}(\mathbf{Q}(\delta))$ is generated by the prime ideals $P \subset R$ such that $N(P) \leq \lfloor \mu \rfloor = 4$. By Lemma 13.8.4, $(2) = P^2$ for $P = (2, 1+\delta)$, and P is not principal. Hence $\langle P \rangle$ has order 2 in $\mathrm{Cl}(\mathbf{Q}(\delta))$. Since $x^2 + 17 \equiv x^2 - 1 = (x+1)(x-1) \mod 3$, we have $(3) = Q\overline{Q}$ for $Q = (3, 1+\delta)$. To find relations among P and Q, we search for elements α of small norm. Taking $\alpha = 1 + \delta$, we have $N(\alpha) = 18 = 2 \cdot 3^2$, so

$$(\alpha)(\overline{\alpha}) = (2) \cdot (3)^2 = P^2 Q^2 \overline{Q}^2.$$

The factorizations of the ideals (α) and $(\overline{\alpha})$ are conjugate to each other and multiply to $P^2 Q^2 \overline{Q}^2$. We have $\alpha \in P$ and $\alpha \in Q$, so both P and Q divide (α), and hence $PQ \mid (\alpha)$. On the other hand, $\alpha = 1 + \delta \notin \overline{Q}$, since otherwise $\overline{Q} \supset Q$ and hence $\overline{Q} = Q$, but (3) does not ramify. Therefore, $(\alpha) = PQ^2$, so taking ideal classes,

$$\langle R \rangle = \langle (\alpha) \rangle = \langle P \rangle \langle Q \rangle^2.$$

This implies $\langle Q \rangle^2 = \langle P \rangle^{-1} = \langle P \rangle$, so $\langle Q \rangle$ has order 4 in $\mathrm{Cl}(\mathbf{Q}(\delta))$ and $\mathrm{Cl}(\mathbf{Q}(\delta))$ is generated by $\langle Q \rangle$. It follows that $\mathrm{Cl}(\mathbf{Q}(\delta))$ is cyclic of order four, and

$$\mathrm{Cl}(\mathbf{Q}(\delta)) = \left\{ \langle R \rangle, \langle Q \rangle, \langle P \rangle, \langle \overline{Q} \rangle \right\}.$$

Problem 4.

Let $f(x) \in \mathbf{Q}[x]$ be an irreducible quartic polynomial with exactly two real roots, let $K \subset \mathbf{C}$ be its splitting field, and let $G = \mathrm{Gal}(K/\mathbf{Q}) \leq S_4$ be its Galois group.

i. Prove that G contains a transposition.

ii. Prove that G is S_4 or D_4.

iii. Find an example of such f where $G = D_4$. [Hint: we saw one in class during an extended example.]

iv. (**Extra credit**) Find an example of such f where $G = S_4$.

Solution.

i. Complex conjugation is an automorphism of K which interchanges the two complex roots of f.

ii. By definition, A_4 is the subgroup of all even permutations of S_4, and $D_2 \leq A_4$. But G contains a transposition, which is an odd permutation. If $G = C_4$ then G is conjugate to $\{e, (1234), (13)(24), (4321)\}$, which does not contain a transposition either. The only remaining transitive subgroups of S_4 are S_4 and D_4.

iii. Let $f(x) = x^4 - 2$. This is irreducible by Eisenstein, and its roots are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$, two of which are real. We have $\mathbf{Q} \subset \mathbf{Q}(\sqrt[4]{2}) \subset \mathbf{Q}(i, \sqrt[4]{2}) = K$, where $[\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}] = 4$ since $x^4 - 2$ is irreducible, and $[\mathbf{Q}(i, \sqrt[4]{2}) : \mathbf{Q}(\sqrt[4]{2})] = 2$ because i is quadratic and $i \notin \mathbf{Q}(\sqrt[4]{2})$. Hence $\#G = 8$, so $G = D_4$ since none of the other possibilities S_4, A_4, C_4, D_2 has 8 elements.

iv. Let $f(x) = x^4 - 2x - 2$. This has two real roots because $f'(x) = 4x^3 - 2$ has exactly one real root and $f(0) = -2 < 0$. It is irreducible by Eisenstein's criterion. Its resolvent cubic equation (cf. Exercise 16.9.9(a)) is

$$g(x) = x^3 + 8x - 4,$$

which is irreducible by the rational root theorem. Hence $G = S_4$.

Problem 5.

Let $d = -23$, let $\delta = \sqrt{-23}$, let $\eta = \frac{1}{2}(1 + \delta)$, and let $R = \mathbf{Z}[\eta]$, the quadratic integer ring in $\mathbf{Q}(\delta)$.

i. Prove that $(2) = P\overline{P}$ for $P = (2, \eta)$.

ii. Prove that P is not principal but P^3 is principal. [Hint: $N(1 + \eta) = 8$.]

iii. Prove that $\text{Cl}(\mathbf{Q}(\delta)) \cong C_3$.

iv. Prove that the cube of every fractional ideal in $\mathbf{Q}(\delta)$ is principal.

Solution.

i. The minimal polynomial $f(x) = x^2 - x + 6$ is congruent to $x(x-1)$ modulo 2, so (2) splits in R. We have $(2) = P\overline{P}$ for $P = (2, \eta)$ since $(2, \eta) \subset R$ corresponds to the ideal $(x) \subset \mathbf{F}_2[x]/(x^2 + x)$.

ii. The element $2 \in R$ is irreducible because $N(\alpha) \geq 6$ for all $\alpha \in \mathbf{Z}[\eta] \setminus \mathbf{Z}$. Hence P is not principal since $P \mid (2)$. As $N(1 + \eta) = 8$, we have

$$(1 + \eta)(1 + \overline{\eta}) = (2)^3 = P^3\overline{P}^3.$$

Hence $(1 + \eta)$ is $P^3, P^2\overline{P}, P\overline{P}^2$, or $\overline{P}^3$. If $(1 + \eta) = P^2\overline{P}$ then $\langle R \rangle = \langle P \rangle^2 \langle \overline{P} \rangle = \langle P \rangle$ since $\langle \overline{P} \rangle = \langle P \rangle^{-1}$, which contradicts the fact that P is not principal. Similarly, $(1 + \eta) \neq P\overline{P}^2$, so either $(1 + \eta) = P^3$ or $(1 + \overline{\eta}) = P^3$.

iii. We know from Theorem 13.7.10 that $\text{Cl}(\mathbf{Q}(\delta))$ is generated by the prime ideals $P \subset R$ such that $N(P) \leq \lfloor \mu \rfloor = 2$. In other words, $\text{Cl}(\mathbf{Q}(\delta))$ is generated by $\langle P \rangle$. We have shown that the order of $\langle P \rangle$ is equal to 3, so $\text{Cl}(\mathbf{Q}(\delta))$ is the cyclic group of order 3 generated by P.

iv. This is a restatement of the fact that the cube of an element of $\text{Cl}(\mathbf{Q}(\delta))$ is trivial.