MATH 371 – Final exam

Please do your own work, and submit your solutions to my mailbox in the math department office by noon on Friday, December 13.

1. Give examples of each of the following, or explain (briefly) why none exists:

(a) A ring R and a prime ideal in R that is not principal.

(b) A ring R and a principal ideal in R that is not prime.

(c) An integral domain that is not a field.

(d) A Euclidean domain that is not a unique factorization domain.

(e) A field F and a polynomial $f \in F[x]$ such that $F[x]/\langle f \rangle$ is not an integral domain.

(f) A field F and a polynomial $f \in F[x]$ such that $F[x]/\langle f \rangle$ is a field with 8 elements.

(g) A field F and a polynomial $f \in F[x]$ such that $F[x]/\langle f \rangle$ is a field with 12 elements.

---

2. Describe the quotient $\mathbb{Z}[i]/\langle 3 \rangle$ as precisely as you can (i.e., what kind of ring is it? is it finite or infinite? if finite, how many elements does it have?). (Here, $\mathbb{Z}[i]$ is the ring of Gaussian integers.) Do the same for $\mathbb{Z}[i]/\langle 5 \rangle$.

---

3. Let R be a ring (commutative, with identity, as usual). R is called a *local ring* if it has a unique maximal ideal.

(a) Prove that if R is a local ring with maximal ideal M then every element $x \in R$ such that $x \notin M$ is a unit.

(b) Conversely, prove that if the set of non-units in the ring R forms an ideal M, then R is a local ring with unique maximal ideal M.

(c) Prove that the set S of all rational numbers m/n such that n is odd (when m/n is in lowest terms) is a ring.

(d) Prove that $\langle 2 \rangle \subset S$ is an ideal, that S is a local ring, and that $\langle 2 \rangle$ is the unique maximal ideal of S.

---

4. Consider the set of 2-by-2 matrices $L = \left\{ \begin{bmatrix} a & b\tau \\ b\tau & a \end{bmatrix} \mid a, b \in \mathbb{Q} \right\}$, where $\tau \in \mathbb{C}$ is *not* a rational number, but τ^2 *is* a rational number.

(a) Show that L is a field.

(b) Show that $\mathbb{Q} \subset L$, and find $[L : \mathbb{Q}]$.

(c) Find an automorphism of L that fixes $\mathbb{Q}$ other than the identity automorphism. How many such automorphisms are there? Is L a Galois extension of $\mathbb{Q}$? If so, what is the Galois group of L over $\mathbb{Q}$?

---

5. Consider the field $F = \mathbb{Q}(\sqrt{2} + \sqrt{5})$.

(a) What is $[F : \mathbb{Q}]$? Find a basis of F as a $\mathbb{Q}$-vector space.

(b) What is the minimal polynomial of $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$?

---

6. Finish up with a few of Brett's problems:

(a) Let R be a (commutative with identity) ring. An element $x \in R$ is *nilpotent* if $x^n = 0$ for some n Show that the set N of all nilpotent elements of R is an ideal of R. Also, show that the quotient ring R/N has no nilpotent elements (other than 0).

(b) Does $x^2 - 3x + 4 \equiv 0 \pmod{97}$ have a solution?

(c) Show that $E = \mathbb{F}_3/\langle x^2 + x + 2 \rangle$ is a field. Calculate $[E : \mathbb{F}_3]$ and find the Galois group $G(E/\mathbb{F}_3)$.

(d) (*Extra credit*:) I have chosen a polynomial $f \in \mathbb{Z}[x]$ with non-negative coefficients but have not told you what it is. I am, however, willing to tell you the result of evaluating f at two integers m and n (where I am willing to tell you $f(m)$ before you choose n, and then I'll tell you $f(n)$). Explain how to choose m and n so that you can identify $f(x)$ based only on this data.