D-MATH
Prof. Brent Doran

Algebra II

FS 2014

# Midterm

## Rings & Fields

This is an open-book exam. You may use any result seen in class or in the exercises without proof. The first exercise is a catalog of questions running through the material on rings and fields. You should be able to answer such questions at the oral exam.

Have fun !

**First part –**

1. A review of the semester.

   (a) Is the quotient of an integral domain necessarily an integral domain ?

   (b) Is the ring $R = \mathbb{Z}[x]/(x^3 + 1, 2)$ actually a field ?

   (c) Find all the ideals of $R$.

   (d) Is $x^5 + 867x^4 + 153x + 351$ irreducible over $\mathbb{Z}$ ?

   (e) Can you find algebraic elements of any degree over $\mathbb{Q}$ ?

   (f) Give an example of a field extension of degree 10.

   (g) Is the regular 7-gon constructible ? What about the regular 8-gon ?

   (h) What is the degree of the splitting field of $x^4 + 4$ over $\mathbb{Q}$ ?

   (i) Consider the rings

   $$\mathbb{Z}/(5) \times \mathbb{Z}/(5), \quad \mathbb{Z}/(25), \quad \mathbb{F}_{25}.$$

   Say which one are fields and which ones are isomorphic to each other.

**Second part –**

2. In this exercise, we compare

   $$R_p = \mathbb{F}_p[x]/(x^2 - 2), \qquad S_p = \mathbb{F}_p[x]/(x^2 - 3).$$

   (a) Exhibit an explicit isomorphism between $R_2$ and $S_2$.

   (b) Prove that $R_5$ is a field, and that it has 25 elements.

   (c) Are $R_5$ and $S_5$ isomorphic ? What about $R_{11}$ and $S_{11}$ ?

3. We give here a direct proof that $\mathbb{Z}[\sqrt{5}]$ is not a unique factorization domain.

(a) Exhibit a factorization of $x^2 + x - 1$ into two linear polynomials over $\mathbb{Q}(\sqrt{5})$.

(b) Prove that $x^2 + x - 1$ is irreducible over $\mathbb{Z}[\sqrt{5}]$.

(c) Conclude that $\mathbb{Z}[\sqrt{5}]$ is not a unique factorization domain.

4. Let $p$ be a prime. We show that $x^p - 2$ is irreducible over $\mathbb{Q}[\zeta_p]$, where $\zeta_p$ denotes the $p$-th root of unity.

   (a) Why is $\left[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}\right] \leqslant p(p-1)$ true ?

   (b) Show that $[\mathbb{Q}[\zeta_p, \sqrt[p]{2}] : \mathbb{Q}] = p(p-1)$.

   (c) Conclude that $x^p - 2$ is irreducible over $\mathbb{Q}[\zeta_p]$.

5. On square roots in finite fields. Let $F$ be a finite field of $q = p^r$ elements. We say that $a \in F$ has a square root if the congruence equation $x^2 \equiv a \bmod q$ has a solution.

   (a) Show that $F^\times \to F^\times, x \mapsto x^2$ is a group homomorphism.

   (b) Show that if $p = 2$ then every element has a square root in $F$.

   (c) Show that, if $p > 2$, the non-zero square roots of $F$ are exactly the solutions to $x^{\frac{q-1}{2}} \equiv 1 \bmod q$. Deduce that $-1$ is a square root in $F$ if and only if $q \equiv 1 \bmod 4$.

   (d) Consider the subfield $K$ generated by $\{x^3 : x \in F\}$. Show that if $K$ is not the whole of $F$, then $F$ must be isomorphic to $\mathbb{F}_4$.