Lecture 12

My handout

Since I wrote the handout, I have nothing more to say about it and think there are sufficient examples for you to study.

Chapter 13

The culmination of the class is really 13.3, Constructability, but we need to learn 13.1 and 13.2 to be able to understand the ideas and proofs in 13.3. By constructability we mean what geometric objects can be constructed by a straightedge and compass. These questions were started by the ancient Greeks who had three unanswered constructability questions that survived to today.

1. Can we construct a square with the same area as a given circle, usually said in shorthand as can we square a circle?
2. Can we trisect every angle? The construction for a bisection is known.
3. Can we construct a cube with double the volume of a given cube, also known as can we double a cube? This question has a story, whose truth is unknown, that Athens was worried about being overrun by the warlike Spartans, so consulted the oracle at Delphi as to what to do. They were told to double the cube that was at the oracle and then they would win. They lost.

By the time we finish 13.3, we will know the answers to these questions, answers that took until Galois answered them sometime between 1830 and 1832 when he died in a duel.

For these sections, instead of Brush up your Shakespeare (song from Kiss Me Kate), please brush up your linear algebra, especially about bases and dimensions.

13.1 Now you may be glad that we did the exercises on characteristic so that the beginning of this section is familiar/known.

Theorem 4 makes formal what we've already found in previous exercises, namely, if $p(x)$ is irreducible in $F[x]$, F a field, then the quotient field $F[x]/(p(x))$ consists of polynomials of lower degree than $p(x)$, i.e., there is a coset representative which is a polynomial of lower degree. That makes $1, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}$ a basis for $F[x]/(p(x))$ over F if the degree of $p(x)$ is n. To make our lives easier, we let θ be any root of $p(x)$ and write our polynomials in θ instead of $\overline{x}$ and our field $F[x]/(p(x))$ as $F(\theta)$ as they are isomorphic. Please notice that it doesn't matter what root of $p(x)$ we pick as we get isomorphic fields.

Some nomenclature may seem redundant. We already have the idea of a subfield, so why say K is an extension field of F if F is a subfield of K? The answer has to do with what field we start with. Before this we started with a big field and looked for subfields. Now we are starting with a field and looking for a bigger field with certain properties. In this section, we want an extension field in which an irreducible polynomial has a root.

Let's see how some of this works out in practice.

13.1.1: $p(x) = x^3 + 9x + 6 \in \mathbb{Q}$ is irreducible by Eisenstein's Irreducibility Criterion with the prime 3. Let θ be a root of $p(x)$. We know that all elements of $\mathbb{Q}(\theta)$ look like $a+b\theta+c\theta^2$ where $\theta^3 = -9\theta-6$. We want to find the inverse of $1+\theta$. So $1 = (1+\theta)(a+b\theta+c\theta^2) = a + (b+a)\theta + (c+b)\theta^2 + c\theta^3 = a - 6c + (b+a-9c)\theta + (b+c)\theta^2$. Therefore $1 = a - 6c,\ b - 9c + a = 0,\ b + c = 0$. Since $b = -c$, we get two equations in two unknowns, namely, $a - 6c = 1,\ a - 10c = 0$. Thus $a = 10c,\ c = 1/4,\ b = -1/4,\ a = 10/4$. So $(1+\theta)^{-1} = (10 - \theta + \theta^2)/4$.

13.1.3: Let $f(x) = x^3 + x + 1$ over $\mathbb{F}_2$. Since $f(0) = 1 = f(1)$, $f(x)$ has no roots in $\mathbb{F}_2$. Since the degree of f is 3, $f(x)$ is irreducible in $\mathbb{F}_2[x]$. Let θ be a root of $f(x)$. Since $0 = \theta^3 + \theta + 1,\ \theta^3 = \theta + 1$ because in characteristic 2, $1 = -1$. Then $\theta^2 = \theta^2,\ \theta^3 = \theta+1,\ \theta^4 = \theta^2+\theta,\ \theta^5 = \theta^3+\theta^2 = \theta^2+\theta+1,\ \theta^6 = \theta^3 + \theta^2 + \theta = \theta^2 + 1,\ \theta^7 = \theta^3 + \theta = 1$.