April 29, 2021

18.702 Comments on Problem Set 10

1. Chapter 15, Exercise 7.6. *(factoring $x^{16} - x$)*

The factors over $\mathbb{F}_2$ are the irreducible polynomials of degrees $1, 2, 4$:

$$x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

The field $\mathbb{F}_8$ has degree 3 over $\mathbb{F}_2$. Therefore none of the factors of degrees 2 or 4 have a root in $\mathbb{F}_8$. Moveover, if one of the factors of degree 4 was a product of quadratic polynomials in $\mathbb{F}_8$, then it would have a root in a quadratic extension of $\mathbb{F}_8$, which would be a field of order $8^2 = 64$. The field $\mathbb{F}_{16}$ isn't contained in $\mathbb{F}_{64}$, so this can't happen. The factorization above is also the irreducible factorization in $\mathbb{F}_8$.

This leaves $\mathbb{F}_4$. The field F_{16} has degree 2 over $\mathbb{F}_4$. In $\mathbb{F}_{16}$, $x^{16} - x$ factors into linear factors. Therefore the irreducible degree four polynomials must be products of quadratic polynomials in $\mathbb{F}_4$.

Let α be a root of x^2+x+1 in $\mathbb{F}_4$. Then the elements of $\mathbb{F}_4$ are $0, 1, \alpha, \beta$, where $\beta = 1+\alpha$. Experimenting with these elements, it isn't hard to find the factorizations. For example, $(x^2+\alpha x+1)(x^2+\beta x+1) = x^4+(\alpha+\beta)x^3+(\alpha\beta)x^2+(\alpha+\beta)+1$. Here $\alpha+\beta = \alpha+1+\alpha = 1$ and $\alpha\beta = \alpha+\alpha^2 = 1$. So this product is $x^4+x^3+x^2+x+1$.

2. Chapter 15, Exercise M4. *(the irreducible polynomial for $\sqrt{2}+\sqrt{3}$)*

(a),(b),(c) are easy. The irreducible polynomial for $\alpha+\beta$, $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$ is the one whose roots are $\pm(\alpha+\beta)$ and $\pm(\alpha-\beta)$.

(d) We note that $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$. The irreducible polynomial for $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ has degree 4. (It is $f(x) = x^4 - 10x^2 + 1$.) If either 2 or 3 is a square, f factors. If not, then 6 will be a square, etc.

3. Prove that, if an element of $GL_2(\mathbb{Z})$ has finite order, then its order is $1, 2, 3, 4$ or 6. Do this by determining the possible characteristic polynomials that such an element could have.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $GL_2(\mathbb{Z})$. We're supposed to knowthat if A has finite order, it is diagonalizable.

The characteristic polynomial of A is $t^2 - (a+d)t + (ad-bc)$, and since A is invertible in the integers, $ad-bc = \pm 1$, while $a+d$ is some integer n. If A has finite order, its eigenvalues will be roots of unity. Let ζ be an eigenvalue. Substituting into the chracteristic polynomial, $\zeta^2 - n\zeta = \zeta(\zeta - n) = \pm 1$. Since ζ and ± 1 have absolute value 1, so does $\zeta - n$, which is difficult since ζ is on the unit circle. It implies that $|n| \le 2$. There are five values of n to consider, and one can look at each one. For example, if $n = 2$, the only possibility is $\zeta = 1$. If $n = 1$, then ζ can be $e^{2\pi 1/6}$ or its inverse, etc.

There are other wasy to reason this out.