18.702 Comments on Problem Set 8

1. Chapter 15, Exercise 3.4. *(the irreducible polynomials for some \( \zeta \))

Let’s do the case of \( \zeta_9 \). Let \( f(x) = x^9 - 1 \), \( \omega = \zeta_9 \) and \( \zeta = \zeta_9 \). We have this factorization over \( \mathbb{Q} \):

\[
f(x) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)
\]

One can show that the sextic factor \( g(x) = x^6 + x^3 + 1 \) is irreducible by showing that it is irreducible modulo 2. It has no root in \( \mathbb{F}_2 \), so if reducible, it would have an irreducible factor of degree 2 or 3. There are only three polynomials to check, to see if they divide \( g \), namely \( x^2 + x + 1 \), \( x^3 + x + 1 \), and \( x^3 + x^2 + 1 \).

Here is a second approach for showing that \( g \) is irreducible modulo 2: In \( \mathbb{F}_2 \), the derivative of \( f(x) = x^9 - 1 \) is \( x^8 \), which doesn’t have a root in common with \( f \). So \( f \) has distinct roots. If \( \alpha \) is any root of \( f \), then \( \alpha^9 = 1 \). Since the roots are distinct, there is a root \( \alpha \) whose order is equal to 9 (not 1 or 3). Then \( \alpha \) is a root of \( g \). If we show that the degree of \( \alpha \) over \( \mathbb{F}_2 \) is 6, it will follow that the irreducible polynomial for \( \alpha \) is \( g \), and therefore that \( g \) is irreducible modulo 2.

We need to show that the field \( \mathbb{F}_2[\alpha] \) has degree 6 over \( \mathbb{F}_2 \), and we know that the order of this field is a power of 2. It will be \( \mathbb{F}_q \), where \( q \) can be one of these numbers: \( q = 4, 8, 16, 32, 64, \ldots \). The multiplicative group \( \mathbb{F}_q^* \) is a cyclic group of order \( q - 1 \). So \( \mathbb{F}_q^* \) contains an element of order 9 if and only if 9 divides \( q - 1 = 1, 3, 7, 15, 31, 63, \ldots \). The first of these integers that is divisible by 9 is 63. Therefore \( q = 64 = 2^6 \), and \( \alpha \) has degree 6 over \( \mathbb{F}_2 \).

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

According to the text, \( x^{16} - x \) splits into linear factors over \( \mathbb{F}_{16} \), and it factors into the irreducible polynomials of degrees 1, 2, 4 over \( \mathbb{F}_2 \). The factorization over \( \mathbb{F}_2 \) is

\[
x^{16} - x = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).
\]

There is a tower of fields \( \mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_{16} \). The degrees of the extensions are

\[
(*) \quad 4 = [\mathbb{F}_{16} : \mathbb{F}_2] = [\mathbb{F}_{16} : \mathbb{F}_4][\mathbb{F}_4 : \mathbb{F}_2] = 2 \cdot 2.
\]

The extension \( \mathbb{F}_4 \) of \( \mathbb{F}_2 \) is generated by a root, call it \( \alpha \), of the quadratic factor. Then \( \mathbb{F}_4 = \{0, 1, \alpha, \beta\} \), where \( \beta = 1 + \alpha \). A root of any one of the quartic factors generates \( \mathbb{F}_{16} \) over \( \mathbb{F}_2 \). Since \( [\mathbb{F}_{16} : \mathbb{F}_4] = 2 \), each quartic factor of \( x^{16} - x \) will be the product of two irreducible quadratic factors in \( \mathbb{F}_4[x] \). It isn’t hard to carry out the factorization in \( \mathbb{F}_4 \) using undetermined coefficients. For example, \( x^4 + x + 1 = (x^2 + x + \alpha)(x^2 + x + \beta) \).

Since \( [\mathbb{F}_8 : \mathbb{F}_2] = 3 \), the smallest field that contains \( \mathbb{F}_{16} \) and \( \mathbb{F}_8 \) is the field of order \( 2^{17} = 128 \). It has degree 4 over \( \mathbb{F}_8 \), so the quartic factors in (*) remain irreducible over \( \mathbb{F}_8 \). Similarly, the quadratic factor remain irreducible.
6. Chapter 15, Exercise M5. (*elements of finite order in GL\(_2(\mathbb{Z})\)*)

By field theory:

Let \( n \) be an integer, and let \( A \) be a matrix with integer entries such that \( A^n = I \). Then the eigenvalues \( \lambda \) also satisfy \( \lambda^n = 1 \). The eigenvalues are roots of the characteristic polynomial, and because \( A \) is an integer matrix, its characteristic polynomial is a quadratic integer polynomial. So we ask: For which \( n \) does an \( n \)th root of unity have degree at most 2 over \( \mathbb{Q} \)? The answer is \( \zeta_1, \zeta_2, \zeta_3, \zeta_4, \) and \( \zeta_6 \). Problem 1 gives a good start at the proof. If \( \zeta_{ab} \) has degree at most 2 over \( \mathbb{Q} \), so does \( \zeta_a = \zeta_{ab} \).

For example, \( \zeta_{10} \) has degree 4.

Using the Crystallographic Restriction:

Let \( G \) be the cyclic group generated by a matrix \( A \) of order \( n \) in \( GL_2(\mathbb{Z}) \). Let \( V = \mathbb{R}^2 \), and let \( T \) be the linear operator on \( V \) whose matrix with respect to the standard basis is \( A \). Because \( A \) has integer entries, \( T \) carries the lattice \( L = \mathbb{Z}^2 \) to itself: \( TL = L \).

Theorem 10.3.6 asserts that there is a \( G \)-invariant, positive definite, symmetric form \(< , > \) on \( V \), a form such that \( < v, w > = < Tv, Tw > \) for all vectors \( v, w \). We change basis in \( V \) to an orthonormal basis for this form, using a real basechange matrix \( P \). The matrix of \( T \) is changed to the real matrix \( A' = P^{-1}AP \), and the lattice \( L \) is no longer the integer lattice in the new coordinates. However, it is still true that \( < v, w > = < Tv, Tw > \). Since the new basis is orthonormal, the new matrix \( A' \) is orthogonal. The property \( TL = L \) remains true too. The Crystallographic Restriction 6.5.12 tells us that \( n = 1, 2, 3, 4, \) or 6.