FINITE MATHEMATICS, PART IIB

IGOR RIVIN

Abstract. We give a short introduction to cyclotomic polynomials, use the to prove Wedderburn's Theorem, and give a short introduction to finite geometries.

1. cyclotomic polynomials

Recall that a *primitive nth root of unity* ω is a complex number such that $\omega^n = 1$, whilst $\omega^m \neq 1$ for any $m < n$. It is not hard to see that if $\omega_n = \exp\left(\frac{2\pi i}{n}\right)$, then the primitive n-th roots of unity are precisely the numbers of the form ω_n^k, where $(n, k) = 1$. It follows that there are $\phi(n)$ primitive n-th roots of unity.

We now define the *n-th cyclotomic polynomial* $\Phi_n(x)$ as

$$\Phi_n(x) = \prod_{\omega \text{ a primitive } n\text{-th root of unity}} (x - \omega).$$

It is not hard to see that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

It follows, by mathematical induction, that $\Phi_n(x)$ is a polynomial with integer coefficients, for every n. Indeed,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, \quad d<n} \Phi_d(x)}.$$

We know that the quotient on the right hand side is without remainder, and the quotient of two polynomials with integer coefficients is a polynomial with integer coefficients.

Theorem 1.1. *Let $q \geq 2$. Then $|\Phi_n(q)| \geq q - 1$, with equality if and only if $n = 1$.*

Date: November 25, 2015.

1991 *Mathematics Subject Classification.* 11R45; 11C08; 11R32.

Key words and phrases. cyclotomic polynomials, Wedderburn's theorem, finite vector spaces and finite geometries.

This is the last part of the course notes for finite mathematics .

Proof. Consider the triangle T in the complex plane whose vertices are $q, 1, \omega = \exp(i\theta)$, for some angle $0 < \theta < \pi$. The angle of T at 1 equals $\pi/2 + \theta/2$, and so, by the Law of Cosines,

$$|q-\exp(i\theta)|^2 = (q-1)^2 + |\exp(i\theta)-1|^2 - 2(q-1)|\exp(i\theta)-1|\cos(\pi/2+\theta/2).$$

Since $\cos(\pi/2 + \theta/2)$ is *negative*, it follows that $q - 1 < |q - \exp(i\theta)|$. Further, since $q \geq 2$, $q - 1 \geq 1$. Now, since $\Phi_n(q)$ is a product of terms of the form $q - \exp(i\theta)$, the result follows. □

2. The Class Equation

Let G be a group. Two elements g, h are said to be *conjugate* in G if there exists $x \in G$, such that $g = x^{-1}hx$. It is fairly clear that conjugacy is an equivalence relation on G (Exercise: prove this). The set of elements conjugate to $g \in G$ is called the *conjugacy class* of g.

Now, define the *center* $Z(G)$ of a group G to be the set of elements $z \in G$ such that $zg = gz$ for every $g \in G$. It is not hard to check that $Z(G)$ is a subgroup of G. It is, similarly, not hard to check that the conjugacy class of every $z \in Z(G)$ has exactly one element. Now, define the *centralizer* of $g \in G$ to be the set $Z_G(g)$ of elements z such that $zg = gz$. The centralizer of an element is easily seen to be a subgroup. Furthermore, we have the following fundamental fact:

Lemma 2.1. *The conjugates of g are in $1-1$ correspondence with the left (or right) cosets of the centralizer of g.*

Proof. Suppose $x^{-1}gx = y^{-1}gy$, for some $x, y \in G$. Then we see that $yx^{-1}g(yx^{-1})^{-1} = g$, so it follows that $yx^{-1} \in Z_G(g)$, and conversely. □

Another easy fact is:

Lemma 2.2. *If g is conjugate to h in G then the centralizer of g is conjugate to the centralizer of h.*

Proof. Indeed, suppose $x^{-1}gx = h$, and $z^{-1}gz = g$. Then,

$$(x^{-1}z^{-1}x)h(x^{-1}zx) = x^{-1}z^{-1}gzx = x^{-1}gx = h.$$

□

An immediate corollary of Lemmas 2.1 and 2.2 for *finite* G is:

Theorem 2.3 (The Class Equation)**.**

$$|G| = \sum_{\text{system of conjugacy classes in } G} \frac{|G|}{|Z_G(g)|}$$

$$= |Z(G)| + \sum_{\text{system of non-central conjugacy classes in } G} \frac{|G|}{|Z_G(g)|},$$

and the quotients on the right hand side do not depend on the system of representatives we pick.

References

School of Mathematics, University of St Andrews, St Andrews, Fife

E-mail address: igor.rivin@st-andrews.ac.uk