Dr. Marques Sophie
Office 519

Number theory

Spring Semester 2014
marques@cims.nyu.edu

Problem Set #10

Recall that if $f(x) \in \mathbb{Z}[x]$ is a non-constant polynomial. Let $P_f = \{p \text{ prime} | \exists n \in \mathbb{N} \text{ such that } p | f(n) \neq 0\}$. Then P_f is infinite. Indeed, assume the contrary and let $p_1, ..., p_k$ be a enumeration of P_f. Choose an integer s so that $f(s) = t \neq 0$; such an s exists as f is non-constant. Now note that

$$f(s + tp_1....p_k w) = f(s) + tp_1...p_k g(x) = t(1 + p_1...p_k g(x))$$

for some $g(x) \in \mathbb{Z}[x]$; in particular $f(s + tp_1...p_k x)$ is divisible by t for any $x \in \mathbb{Z}$. Now consider $h(x) := \frac{1}{t} f(s + tp_1...p_k x) = 1 + p_1...p_k x) = 1 + p_1...p_k g(x)$. But h is non-constant, so we may choose $u \in \mathbb{Z}$ with $h(u) \neq 1$. So $h(u) \equiv 1 \ mod \ p_1...p_k$, and thus $h(u)$ is divisible by some prime $p \neq p_i$ for $i = 1, ..., k$. But then $p \in P_f$, which is a contradiction.

Exercise 1 p 64 (Dirichlet's Prime Number Theorem)
For every natural number n there are infinitely many prime numbers $p \equiv 1 \ mod \ n$.

Solution:
Let $\phi_n(x) \in \mathbb{Z}[x]$ be the n-th cyclotomic polynomial, that is the minimal polynomial of a primitive n-th root of unity ξ_n over $\mathbb{Q}$.
Let $a \in \mathbb{Z}$ and consider p prime with $p | \phi_n(a) \neq 0$ where $p \nmid n$. Let m be the order of a mod p; we claim that $n = m$. Indeed $\phi_n | (x^n - 1)$, so $p | a^n - 1$ and thus $m | n$. Assume $m < n$. But then $p | \phi_n(a)$, $a^m - 1$; but both $\phi_n(x)$, $x^m - 1$ divide $x^n - 1$ and the two polynomials are relatively prime mod p (indeed, the former is irreducible and does not divide the latter), so $x^n - 1$ has a double root mod p at a. But the discriminant of $x^n - 1$ is n^n, which is non-zero mod p (as $p \nmid n$) so this is a contradiction. So we must have $m = n$. But note that $a^{p-1} \equiv 1 \ mod \ p$, so $n | p - 1$, and thus $p \equiv 1 \ mod \ n$. So any prime is $P_{\phi_n(x)}$ either divides n or satisfies $p \equiv 1 \ mod \ n$. But, by the reminder above the exercise, there are infinitely many primes in $P_{\phi_n(x)}$, and only finitely many prime divide n, so there are infinitely many primes satisfying $p \equiv 1 \ mod \ n$.

Exercise 2 p 65
For evert finite abelian group A there exists a Galois extension $L|\mathbb{Q}$ with Galois group $G(L|\mathbb{Q}) \simeq A$. (We will prove that there is infinitely many such extension).

Solution:
This will first be proven for G cyclic.
Let $|G| = n$. By Dirichlet's theorem on primes in arithmetic progressions, there exists a prime p with $p \equiv 1 \ mod \ n$. Let ξ_p denote a primitive p^{th} root of unity. Let $L = \mathbb{Q}(\xi_p)$. Then $L/\mathbb{Q}$ is Galois with $Gal(L/\mathbb{Q})$ cyclic of order $p - 1$. Since n divides p?1, there exists a subgroup H of $Gal(L/\mathbb{Q})$ such that $|H| = \frac{p-1}{n}$. Since $Gal(L/\mathbb{Q})$ is cyclic, it is

abelian, and H is a normal subgroup of $Gal(L/\mathbb{Q})$. Let $K = L^H$, the subfield of L fixed by H. Then $K/\mathbb{Q}$ is Galois with $Gal(K/\mathbb{Q})$ cyclic of order n. Thus, $Gal(K/\mathbb{Q})?G$.
Let p and q be distinct primes with $p \equiv 1$ mod n and $q \equiv 1$ mod n. Then there exist subfields K_1 and K_2 of $\mathbb{Q}(\xi_p)$ and $\mathbb{Q}(\xi_q)$, respectively, such that $Gal(K_1/\mathbb{Q}) \simeq G$ and $Gal(K_2/\mathbb{Q}) \simeq G$. Note that $K_1 \cap K_2 = \mathbb{Q}$ since $\mathbb{Q} \subseteq K_1 \cap K_2 \subseteq \mathbb{Q}(\xi_p) \cap \mathbb{Q}(\xi_q) = \mathbb{Q}$. Thus, $K_1 \neq K_2$. Therefore, for every prime p with $p \equiv 1$ mod n, there exists a distinct number field K such that $K/\mathbb{Q}$ is Galois and $Gal(K/\mathbb{Q}) \simeq G$. The theorem in the cyclic case follows from using the full force of Dirichlet's theorem on primes in arithmetic progressions: There exist infinitely many primes p with $p \equiv 1$ mod n.
The general case follows immediately from the above argument, the fundamental theorem of finite abelian groups, and a theorem regarding the Galois group of the compositum of two Galois extensions.

Exercise 3 p 65
Every quadratic number field $\mathbb{Q}(\sqrt{d})$ is contained in some cyclotomic field $\mathbb{Q}(\xi_n)$, ξ_n a primitive n^{th} root of unity.

Solution:
Since $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\xi_m)$ and $\mathbb{Q}(\sqrt{b}) \subseteq \mathbb{Q}(\xi_n)$, then $\mathbb{Q}(\sqrt{ab}) \subseteq \mathbb{Q}(\sqrt{a}, \sqrt{b}) \subseteq \mathbb{Q}(\xi_m, \xi_n) \subseteq \mathbb{Q}(\xi_{mn})$, so in order to prove the general statement it is enough to prove that:

1. *$\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\xi_4)$;*
2. *$\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\xi_8)$ and $\mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\xi_8)$.*
3. *If p is a prime congruent to 1 modulo 4,then $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\xi_p)$.*
4. *If p is a prime congruent to 3 modulo 4, then $\mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\xi_p)$.*

1. *is obvious.* 2. *come from the fact that $\xi_8 = (1+i)/\sqrt{2}$. We have proven, p 51 that if τ is the Gauss sum $\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{a}{p}\right)\xi^a$, then $\tau^2 = \left(\frac{-1}{p}\right)p = p^*$ and*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} -1 & p \equiv 3 \text{ mod } 4 \\ 1 & p \equiv 1 \text{ mod } 4 \end{cases}$$

(Note that for p prime, $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic field intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\xi_p)$. Indeed, $Gal(\mathbb{Q}(\xi_p), \mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ contains a unique subgroup of index two, so there is a unique quadatic field intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\xi_p)$ and we have just identified that field.)

Exercise 3, 4, 5 p 65

4. Describe the quadratic subfields of $\mathbb{Q}(\xi_n)|\mathbb{Q}$ in the case where n is odd.
5. Show that $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ are the quadratic subfield of $\mathbb{Q}(\xi_n)|\mathbb{Q}$ for $n = 2^q$, $q \geq 3$.

Solution:
We will prove 4. and 5. proving that more generally that if $n > 2$ is an integer. Define $A = \{a_i\}_{i=1,\ldots,t}$ as follows: if p is an odd prime factor of n, then $p^* \in A$. If n is

divisible by 4, *then* $-1 \in A$. *If* n *is divisible by* 8, *then* $2 \in A$. *Then* $\mathbb{Q}(\xi_n)$ *contains* $2^t - 1$ *quadratic extensions of* $\mathbb{Q}$ *and they are* $\mathbb{Q}(\sqrt{m})$ *for* m *any nontrivial product of distinct elements of* A.
By the fundamental Theorem of Galois Theory, the quadratic extensions of $\mathbb{Q}$ *contained in* $\mathbb{Q}(\xi_n)$ *are in* $1-1$ *correspondence with the subgroups of index* 2 *of* $Gal(\mathbb{Q}(\xi_n), \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. *Now if* $n = 2^{e_2}3^{e_3}5^{e_5}...$,

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/2^{e_2}\mathbb{Z})^* \times (\mathbb{Z}/3^{e_3}\mathbb{Z})^* \times (\mathbb{Z}/5^{e_5}\mathbb{Z})^* \times ....$$

For p *odd and* $k \geq 1$, $(\mathbb{Z}/p^k\mathbb{Z})^*$ *is a cyclic group of even order. Also,* $(\mathbb{Z}/2\mathbb{Z})^*$ *is trivial,* $(\mathbb{Z}/4\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z})$, *and* $(\mathbb{Z}/2^k\mathbb{Z})^* \simeq ((\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2^{k-2}\mathbb{Z})$. *Thus* $(\mathbb{Z}/n\mathbb{Z})^*$ *contains* $2^t - 1$ *subgroups of index* 2. *(A subgroup of index* 2 *is the kernel of an epimorphism* $\psi : Gal(\mathbb{Q}(\xi_n), \mathbb{Q}) \to \mathbb{Z} = 2\mathbb{Z}$ *and since* $Gal(\mathbb{Q}(\xi_n), \mathbb{Q})$ *is isomorphic to the direct sum of* t *cyclic group of even order, there are* 2^t *homomorphism from* $Gal(\mathbb{Q}(\xi_n), \mathbb{Q})$ *to* $\mathbb{Z}/2\mathbb{Z}$, *one of which is the trivial one.) Since* $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\xi_n)$ *for each of the* $2^t - 1$ *values of* m *in* A, *by the previous exercise, we see that these are all the quadratic subfields of* $\mathbb{Q}(\xi_n)$.