Solutions 13

Analytic class number formula, density

1. Determine the Dirichlet density of the set of rational primes $p \equiv 3 \bmod (4)$ that split completely in the field $\mathbb{Q}(\sqrt[3]{2})$.

   Solution: On the one hand put $K := \mathbb{Q}(\sqrt[3]{2})$, so that $M := \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ is a galois closure of $K/\mathbb{Q}$. Then by exercise 1 of sheet 9 a prime number is totally split in $\mathcal{O}_K$ if and only if it is totally split in $\mathcal{O}_M$. On the other hand put $L := \mathbb{Q}(i)$. Then by exercise 2 of sheet 8 an odd prime number p is non-split in $\mathcal{O}_L$ if and only if $p \equiv 3 \bmod (4)$. Thus, we want the set of primes that split totally in $\mathcal{O}_M$ but not in $\mathcal{O}_L$. By Proposition 7.5.5, this means that they split in M but not in ML. By Propositions 7.5.4 and 7.5.5 the desired Dirichlet density is therefore

   $$\frac{1}{[M/\mathbb{Q}]} - \frac{1}{[ML/\mathbb{Q}]} = \frac{1}{6} - \frac{1}{12} = \frac{1}{12}.$$

   Aliter: The fields M and L are linearly disjoint galois extensions of $\mathbb{Q}$; hence $ML/\mathbb{Q}$ is galois with Galois group $\mathrm{Gal}(M/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \cong S_3 \times S_2$. Aside from finitely many ramified primes, we want the set of rational primes p whose associated Frobenius element in $\mathrm{Gal}(ML/\mathbb{Q})$ is equal to $(1, \sigma)$ for $1 \neq \sigma \in S_2$. This element is alone in its conjugacy class, hence by the Cebotarev density theorem the set in question has Dirichlet density $1/|\mathrm{Gal}(ML/\mathbb{Q})| = 1/12$.

2. Let L/K be an extension of number fields. Prove that $L = K$ if and only if the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ which are totally split in L has Dirichlet density $> \frac{1}{2}$.

   Solution: If $L = K$, then all primes of $\mathcal{O}_K$ are totally split in $\mathcal{O}_L$ by definition. Conversely, let M denote the galois closure of L/K. By exercise 1 of sheet 8 a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is totally split in $\mathcal{O}_L$ if and only if it is totally split in $\mathcal{O}_M$. By Proposition 7.5.4 we therefore have

   $$\mu(S_{L/K}) = \mu(S_{M/K}) = \frac{1}{[M/K]} \leqslant \frac{1}{[L/K]}.$$

   Thus if $\mu(S_{L/K}) > \frac{1}{2}$, we have $[L/K] < 2$ and hence $L = K$.

3. Let L/K be an extension of number fields. Prove that L/K is galois if and only if for almost all primes $\mathfrak{p} \subset \mathcal{O}_K$, if there exists a prime $\mathfrak{P}|\mathfrak{p}$ of $\mathcal{O}_L$ with $f_{\mathfrak{P}/\mathfrak{p}} = 1$, then $\mathfrak{p}$ is totally split in $\mathcal{O}_L$.

Solution: As in the lecture, let $S_{L/K}$ be the set of non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which are totally split in $\mathcal{O}_L$. Let $P_{L/K}$ be the set of non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ for which there exists a prime $\mathfrak{P}|\mathfrak{p}$ of $\mathcal{O}_L$ with $f_{\mathfrak{P}/\mathfrak{p}} = 1$. Then we must show that L/K is galois if and only if the set $X_{L/K} := P_{L/K} \smallsetminus S_{L/K}$ is finite.

If L/K is galois, for all primes $\mathfrak{p} \subset \mathcal{O}_K$ we have $[L/K] = r_\mathfrak{p} e_\mathfrak{p} f_\mathfrak{p}$; hence $S_{L/K}$ is the set of $\mathfrak{p}$ with $e_\mathfrak{p} f_\mathfrak{p} = 1$, and $P_{L/K}$ is the set of $\mathfrak{p}$ with $f_\mathfrak{p} = 1$. Thus $X_{L/K}$ is contained in the finite set of $\mathfrak{p}$ with $e_\mathfrak{p} > 1$ and is therefore itself finite.

Conversely, suppose that L/K is not galois. Let M/K be its galois closure. Then M/L is a proper galois extension. By Proposition 7.5.4 the set $S_{M/L}$ of primes of $\mathcal{O}_L$ which are totally split in $\mathcal{O}_M$ thus has Dirichlet density $\frac{1}{[M/L]} < 1$. Its complement A therefore has Dirichlet density $1 - \frac{1}{[M/L]} > 0$, and by Proposition 7.5.2 so does the subset of primes in A of absolute degree 1. Thus there exist infinitely many primes $\mathfrak{P} \subset \mathcal{O}_K$ of absolute degree 1 which are not totally split in $\mathcal{O}_M$. But any such $\mathfrak{P}$ has residue degree $f_{\mathfrak{P}/\mathfrak{p}} = 1$, hence the corresponding prime $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ lies in $X_{L/K}$. Thus the set $X_{L/K}$ is infinite, as desired.

4. Let a be an integer that is not a third power. Let A be the set of prime numbers p such that a mod (p) is a third power in $\mathbb{F}_p$.

   (a) Prove that A and its complement are both infinite.

   (b) Prove that there is no integer N such that the property $p \in A$ depends only on the residue class of p modulo (N).

Solution: By assumption the cubic polynomial $X^3 - a$ does not have a root in $\mathbb{Z}$; hence by the Gauss lemma also not in $\mathbb{Q}$; so it is irreducible. Thus the field $K := \mathbb{Q}(\sqrt[3]{a})$ is isomorphic to $\mathbb{Q}[X]/(X^3 - a)$, and its ring of integers $\mathcal{O}_K$ contains the subring $\mathcal{O} := \mathbb{Z}[\sqrt[3]{a}] \cong \mathbb{Z}[X]/(X^3 - a)$. Since both $\mathcal{O} \subset \mathcal{O}_K$ are free $\mathbb{Z}$-modules of rank 3, the index $d := [\mathcal{O}_K : \mathcal{O}]$ is finite. Thus for any prime $p \nmid d$ we obtain a natural isomorphism

$$\mathbb{F}_p[X]/(X^3 - a) \;\cong\; \mathcal{O}/p\mathcal{O} \;\xrightarrow{\sim}\; \mathcal{O}_K/p\mathcal{O}_K.$$

For any such p it follows that $p \in A$ if and only if there exists a homomorphism $\mathcal{O}_K/p\mathcal{O}_K \to \mathbb{F}_p$, that is, if and only if there exists a prime $\mathfrak{p}|p$ of $\mathcal{O}_K$ with $f_{\mathfrak{p}/p} = 1$.

Next, the ratio of two distinct roots of $X^3 - a$ is a primitive third root of unity ζ_3, hence the galois closure of $K/\mathbb{Q}$ is $\tilde{K} := KL$ with the imaginary quadratic field $L := \mathbb{Q}(\zeta_3)$. Moreover $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \cong S_3$ with the normal subgroup $\mathrm{Gal}(\tilde{K}/L) \cong A_3$.

(a) Since $\tilde{K}/\mathbb{Q}$ is galois of degree 6, by Proposition 7.5.4 the set of rational primes that are totally split in $\mathcal{O}_{\tilde{K}}$ has Dirichlet density $\frac{1}{6}$; in particular it is infinite. These primes are also totally split in the intermediate field K; hence by the above remarks almost all of them lie in A. Thus A is infinite.

On the other hand, since $L/\mathbb{Q}$ is galois of degree 2, the same proposition shows that the set of rational primes that split in $\mathcal{O}_L$ has Dirichlet density $\frac{1}{2}$. As this set contains the set of primes that are totally split in $\mathcal{O}_{\tilde{K}}$, it follows that the set of rational primes that are totally split in $\mathcal{O}_L$ but not in $\mathcal{O}_{\tilde{K}}$ has Dirichlet density $\frac{1}{2} - \frac{1}{6} = \frac{1}{3}$. In particular there are infinitely many such p. For each of these the decomposition group at any prime $\tilde{\mathfrak{p}} \subset \mathcal{O}_{\tilde{K}}$ above p is non-trivial, but acts trivially on L; hence it is equal to $\mathrm{Gal}(\tilde{K}/L) \cong A_3$. Since $\mathrm{Gal}(\tilde{K}/K) \cong S_2 < S_3$ and $S_3 = S_2 \cdot A_3$, by exercise 1 (b) on sheet 9 it follows that there is only one prime $\mathfrak{p} \subset \mathcal{O}_K$ above p. As only finitely many primes are ramified in $\mathcal{O}_K$, for all the other such p we must have $f_{\mathfrak{p}/p} = 3$. By the above remarks almost all of these p thus lie in the complement of A, which is therefore also infinite.

(b) If there is such an N, we can without loss of generality assume that $3|N$, so that L is contained in the cyclotomic field $\hat{L} := \mathbb{Q}(\mu_N)$. Then $\hat{K} := K\hat{L}$ is galois of degree 3 over $\hat{L}$. Since $\hat{L}/\mathbb{Q}$ is galois of degree $\varphi(N)$, the extension $\hat{K}/\mathbb{Q}$ is galois of degree $3\varphi(N)$. By the same arguments as in (a) applied to $\hat{K}/\hat{L}/\mathbb{Q}$ instead of $\tilde{K}/L/\mathbb{Q}$ we find that of the rational primes which are totally split in $\mathcal{O}_{\hat{L}}$, infinitely many lie in A and infinitely many in the complement of A. But by Example 6.5.5 the rational primes which are totally split in $\mathcal{O}_{\hat{L}}$ are precisely those that are congruent to 1 modulo (N). Thus the congruence class $p \bmod (N)$ does not determine whether $p \in A$ or not; hence such N cannot exist.

*5. For $d, N \geqslant 1$, consider the set $P_{d,N}$ of polynomials in one variable of degree at most d whose coefficients have absolute value $\leqslant N$. Consider the subset $Q_{d,N}$ of those polynomials whose Galois group over $\mathbb{Q}$ is the symmetric group S_d. Prove that $\lim_{N\to\infty} \frac{|Q_{d,N}|}{|P_{d,N}|} = 1$.

Hint: Look at the factorization of polynomials modulo prime numbers.

Solution: For the first known proof see [van der Waerden, B. L.: Die Seltenheit der Gleichungen mit Affekt. (German) *Math. Ann.* **109** (1934), no.1, 13–16.] `https://mathscinet.ams.org/mathscinet/article?mr=1512878`

6. Consider an integer $m \geqslant 1$ and let $L \subset \mathbb{Q}(\mu_m)$ be the intermediate field corresponding to a subgroup $\Gamma < (\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$. Express the zeta function $\zeta_L(s)$ as a product of Dirichlet L-functions.

Solution: Let X_L be the set of homomorphisms $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ with $\chi|\Gamma = 1$. For any $\chi \in X_L$ let χ_{prim} be the associated primitive Dirichlet character of modulus dividing m. We claim that $\zeta_L(s)$ is the product of the L-functions $L(\chi_{\mathrm{prim}}, s)$ for all $\chi \in X_L$.

Since

$$\zeta_L(s) \;=\; \prod_{\mathfrak{p}} \big(1 - \mathrm{Nm}(\mathfrak{p})^{-s}\big)^{-1} \;=\; \prod_{p} \prod_{\mathfrak{p}|p} \big(1 - \mathrm{Nm}(\mathfrak{p})^{-s}\big)^{-1}$$

and

$$L(\chi_{\rm prim}, s) \;=\; \prod_p \big(1 - \chi_{\rm prim}(p) p^{-s}\big)^{-1}$$

it suffices to prove for every fixed p that

$$\prod_{\mathfrak{p}|p} \big(1 - \mathrm{Nm}(\mathfrak{p})^{-s}\big) \;=\; \prod_{\chi \in X_L} \big(1 - \chi_{\rm prim}(p) p^{-s}\big). \tag{$*$}$$

To achieve this, recall from Proposition 6.3.4 that the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ above p satisfy $p\mathcal{O}_L = \mathfrak{p}_1^e \cdots \mathfrak{p}_r^e$ with $[k(\mathfrak{p}_i)/\mathbb{F}_p] = f$ for all i and $[L:\mathbb{Q}] = ref$. Thus $\mathrm{Nm}(\mathfrak{p}_i) = p^f$ for all i; hence the left hand side of $(*)$ is equal to $(1 - p^{-fs})^r$. Abbreviating $T = p^{-s}$, we are therefore reduced to showing that

$$(1 - T^f)^r \;=\; \prod_{\chi \in X_L} \big(1 - \chi_{\rm prim}(p) T\big). \tag{$**$}$$

Suppose first that $p \nmid m$. Then p is unramified in $\mathbb{Q}(\mu_m)$ and hence also in L. Thus $e = 1$. Also, by Example 6.5.5 the Frobenius substitution at p for the extension $\mathbb{Q}(\mu_m)/\mathbb{Q}$ corresponds to the residue class $\bar{p}$ under the isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. The Frobenius substitution at p for $L/\mathbb{Q}$ thus corresponds to the image $[\bar{p}]$ of $\bar{p}$ in the factor group $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times/\Gamma$. Moreover f and r are then simply the order and the index of the subgroup $\langle[\bar{p}]\rangle$.

Now observe the following elementary facts from group theory:

Lemma 1: For any finite abelian group G there are precisely $|G|$ different homomorphisms $G \to \mathbb{C}^\times$.

Proof: By the structure theorem for finite abelian groups there is an isomorphism $G \cong \prod_{i=1}^r \mathbb{Z}/e_i\mathbb{Z}$. Any homomorphism must map the generator of the i-th factor to an e_i-th root of unity, and conversely, any choice of an e_i-th root of unity for every i extends uniquely to a homomorphism $G \to \mathbb{C}^\times$. The number of homomorphisms is therefore $\prod_{i=1}^r e_i = |G|$. □

Lemma 2: For any finite abelian group G and any subgroup G', every homomorphism $G' \to \mathbb{C}^\times$ possesses precisely $[G:G']$ different extensions to a homomorphism $G \to \mathbb{C}^\times$.

Proof: First note that for any two homomorphisms $G \to \mathbb{C}^\times$ the quotient is again a homomorphism, and two homomorphisms coincide on G' if and only if their quotient is trivial on G'. On the other hand, applying Lemma 1 to the factor group G/G' shows that there are precisely $|G/G'|$ different homomorphisms $G \to \mathbb{C}^\times$ which are trivial on G'. Combining these statements shows that for every homomorphism $G \to \mathbb{C}^\times$, there are precisely $|G|/|G'|$ homomorphisms (including the given one) which have the same restriction to G'. Since the total number of homomorphisms $G \to \mathbb{C}^\times$ is $|G|$ by Lemma 1, these homomorphisms therefore decompose into $|G'|$ sets of size $|G|/|G'|$ with the same restriction to G'. As the number of homomorphisms $G' \to \mathbb{C}^\times$ is already $|G'|$ by Lemma 1, it follows that each of these extends in precisely $|G|/|G'|$ ways to a homomorphism $G \to \mathbb{C}^\times$. $\square$

Applying these lemmas, note that by Lemma 1 there are precisely f homomorphisms $\langle[\bar{p}]\rangle \to \mathbb{C}^\times$, mapping the generator $[\bar{p}]$ to the f distinct f-th roots of unity. By Lemma 2 each of these possesses precisely $[L/K]/f = r$ different extensions to a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times/\Gamma \to \mathbb{C}^\times$. But giving a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times/\Gamma \to \mathbb{C}^\times$ is equivalent to giving a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ which vanishes on Γ. Thus by the definition of X_L, for every homomorphism $\chi \in X_L$ the element $\chi(\bar{p}) \in \mathbb{C}^\times$ is an f-th root of unity, and conversely, for every f-th root of unity ζ there are precisely r homomorphisms $\chi \in X_L$ with $\chi(\bar{p}) = \zeta$. Together this shows that

$$\prod_{\chi \in X_L} \big(1 - \chi(p)T\big) \;=\; \prod_{\zeta \in \mu_f} (1 - \zeta T)^r \;=\; (1 - T^f)^r$$

is equal to the left hand side of $(**)$. Finally, since p is coprime to m, for every $\chi \in X_L$ we have $\chi(p) = \chi_{\mathrm{prim}}(p)$. This proves the equality $(**)$ in the case $p \nmid m$.

Now suppose that $p|m$ and write $m = p^k m'$ with $p \nmid m'$. Then $\mathbb{Q}(\mu_m)$ is generated by the linearly disjoint extensions $\mathbb{Q}(\mu_{p^k})$ and $\mathbb{Q}(\mu_{m'})$ of $\mathbb{Q}$, and the induced isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_{p^k})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_{m'})/\mathbb{Q})$ corresponds to the isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/p^k\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times$ from the Chinese remainder theorem. As p is totally ramified in $\mathbb{Q}(\mu_{p^k})$ and unramified in $\mathbb{Q}(\mu_{m'})$, the inertia group above p is precisely the subgroup $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_{m'}))$ which corresponds to the factor $(\mathbb{Z}/p^k\mathbb{Z})^\times \times \{1\}$ of the latter group.

Passing to L the main theorem of Galois theory implies that the image of the inertia group $(\mathbb{Z}/p^k\mathbb{Z})^\times \times \{1\}$ in $(\mathbb{Z}/m\mathbb{Z})^\times/\Gamma$ corresponds to the subfield $L' := L \cap \mathbb{Q}(\mu_{m'})$, whose associated subgroup $\Gamma' < (\mathbb{Z}/m'\mathbb{Z})^\times$ is precisely the image of Γ. This shows that p is unramified in $\mathcal{O}_{L'}$ and that every prime $\mathfrak{p}'$ of $\mathcal{O}_{L'}$ above p is totally ramified in $\mathcal{O}_L$. Thus the primes of $\mathcal{O}_{L'}$ above p are in bijection with those of $\mathcal{O}_L$ and have the same residue field. The left hand side of $(**)$ for $L \subset \mathbb{Q}(\mu_m)$ is therefore equal to that for $L' \subset \mathbb{Q}(\mu_{m'})$. We have already seen that the latter is equal to

$$\prod_{\chi \in X_{L'}} \big(1 - \chi_{\mathrm{prim}}(p)T\big).$$

By the definition of X_L and $X_{L'}$ this in turn is equal to

$$\prod_{\substack{\chi \in X_L \\ \chi \text{ trivial on } (\mathbb{Z}/p^k\mathbb{Z})^\times \times \{1\}}} \big(1 - \chi_{\mathrm{prim}}(p)T\big).$$

Finally, for every $\chi \in X_L$ which is non-trivial on $(\mathbb{Z}/p^k\mathbb{Z})^\times \times \{1\}$, the modulus of the associated primitive character χ_{prim} is divisible by p, which implies that $\chi_{\text{prim}}(p) = 0$. Thus the two sides of $(**)$ are also equal in the case $p|m$, and we are done.