D-MATH
Prof. Richard Pink

Algebraic Number Theory

FS 2018

Solutions 14

Dirichlet Density, Primes in Arithmetic Progressions

1. Does there exist a number field which does not embed into $\mathbb{Q}_p$ for any p?

   Solution: The answer is no. In fact for every number field K, there are infinitely many prime numbers p such that K embeds into $\mathbb{Q}_p$. To show this, let M denote the galois closure of $K/\mathbb{Q}$. Then by §17 Proposition 5, the set of primes p which split completely in M has Dirichlet density $\frac{1}{[M/\mathbb{Q}]}$ and is therefore infinite. For any such p, let $\mathfrak{p} \subset \mathcal{O}_M$ be a prime above p. Then the decomposition group of $\mathfrak{p}/p$ is trivial; hence by §13 Proposition 8 the corresponding extension of local fields $M_\mathfrak{p}/\mathbb{Q}_p$ is galois with trivial galois group. Thus $M_\mathfrak{p} = \mathbb{Q}_p$, and the composite $K \hookrightarrow M \hookrightarrow M_\mathfrak{p} = \mathbb{Q}_p$ is the desired embedding.

2. Determine the Dirichlet density of the set of 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 §6 Proposition 12 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 3 of sheet 4 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 §17 Lemma 6, this means that they split in M but not in ML. By §17 Propositions 1 (f) and 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 $1/|\,\mathrm{Gal}(ML/\mathbb{Q})| = 1/12$.

3. 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 §6 Proposition 12, 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 §17 Proposition 5 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 $L = K$.

4. 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 §17 Proposition 5 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 §17 Proposition 3 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.

5. Let a be an integer that is not a third power. Let A be the set of prime numbers p such that $a \bmod (p)$ 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 §17 Proposition 5 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 §6 Proposition 11 (c) 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 §8 Proposition 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.