

Galois Theory Problem Set 3

Austin Mohr

December 10, 2009

1 Problem 17

Proposition 1.1. *Let R be a real closed field and let $f(x) \in R[x]$. Suppose that $a < b$ in R and that $f(a)f(b) < 0$. There is $c \in R$ with $a < c < b$ such that c is a root of $f(x)$.*

Proof. Assume $f(x)$ is monic, and so $f(x) = (x - r_0)(x - r_1) \cdots (x - r_m)g_1(x) \cdots g_s(x)$ with $g_i(x) = x^2 + c_i x + d_i$ and $c_i^2 < 4d_i$. It follows that

$$\begin{aligned} g_i(x) &= \left(x + \frac{c_i}{2}\right)^2 + \frac{1}{4}(4d_i - c_i^2) \\ &= \left(x + \frac{c_i}{2}\right)^2 + e_i^2, \end{aligned}$$

where $e_i^2 = \frac{1}{2}\sqrt{4d_i - c_i^2}$. Now, $g_i(u) > 0$ for all $u \in R$. If $a < r_i$ and $b < r_i$ for all $1 \leq i \leq m$, then $f(a)f(b) = (a - r_i)(b - r_i)g_j(a)g_j(b) > 0$. Similarly, if $a > r_i$ and $b > r_i$ for all $1 \leq i \leq m$, then $f(a)f(b) > 0$. Since $f(a)f(b) < 0$, it follows that either $a < r_j < b$ or $b < r_j < a$ for some $1 \leq j \leq m$. As r_j is a root of f , we take r_j to be c . \square

2 Problem 18

Proposition 2.1. *Let R be a real closed field, let $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n = f(x) \in R[x]$, and put $M = |a_0| + |a_1| + \cdots + |a_{n-1}| + 1$. Every root of $f(x)$ that belongs to R belongs to the interval $[-M, M]$.*

Proof. Let r be any root of f . Since $|M| \geq 1$, we can assume $|r| > 1$ (otherwise, we are already finished). Now,

$$\begin{aligned} f(r) &= a_0 + a_1 r + \cdots + a_{n-1} r^{n-1} + r^n \\ &= r^n \left(\frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} + 1 \right). \end{aligned}$$

As r is a root f ,

$$\begin{aligned}
0 &= r^n \left(\frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} + 1 \right) \\
0 &= \frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} + 1 \\
-1 &= \frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} \\
1 &= \left| \frac{a_0}{r^n} + \frac{a_1}{r^{n-1}} + \cdots + \frac{a_{n-1}}{r} \right| \\
1 &\leq \left| \frac{a_0}{r^n} \right| + \left| \frac{a_1}{r^{n-1}} \right| + \cdots + \left| \frac{a_{n-1}}{r} \right| \\
1 &\leq \left| \frac{a_0}{r} \right| + \left| \frac{a_1}{r} \right| + \cdots + \left| \frac{a_{n-1}}{r} \right| \\
|r| &\leq |a_0| + |a_1| + \cdots + |a_{n-1}| \\
|r| &\leq M,
\end{aligned}$$

as desired. □

3 Problem 19

Proposition 3.1. *Every element of a finite field can be written as the sum of two squares.*

Proof. Let F be a finite field having characteristic p and $|F| = p^n$. Define $\phi : F \rightarrow F$ by $\phi(x) = x^2$. If $p = 2$, then ϕ is an isomorphism, and so for any $u \in F$ there is $v \in F$ with $u = v^2 + 0^2$. If $p > 2$, then for all $x, y \in F$, $x^2 = y^2$ implies that $(x + y)(x - y) = 0$. Hence, $y = x$ or $y = -x$, and so $|Im\phi| \geq \frac{p^n+1}{2}$. Let $m = \frac{p^n+1}{2}$ and choose distinct elements x_1^2, \dots, x_m^2 in F . Hence, for any $u \in F$ and for all $1 \leq i \leq m$, $u - x_i^2$ are distinct elements in F . Since $2m > p^n$, there exists j and k such that $x_j^2 = u - x_k^2$. That is, $u = x_j^2 + x_k^2$, as desired. □

4 Problem 20

Proposition 4.1. *Every polynomial with rational coefficients that has a splitting field of dimension 1225 over the rationals is solvable by radicals.*

Proof. Let E be a splitting field of dimension 1225 over the rationals. A polynomial with rational coefficients is solvable by radicals if and only if $\text{Gal}(E/\mathbb{Q})$ is solvable. We argue that $\text{Gal}(E/\mathbb{Q})$ is Abelian, and hence solvable, as every Abelian group is solvable.

Let $G = \text{Gal}(E/\mathbb{Q})$. Observe first that $1225 = 5^2 7^2$. Consider the Sylow p -subgroups of G . Sylow's theorem gives

- $n_5 \equiv 1 \pmod{5}$ and $n_5 \mid 49$, so $n_5 = 1$
- $n_7 \equiv 1 \pmod{7}$ and $n_7 \mid 25$, so $n_7 = 1$

Hence, \mathbf{G} has a unique Sylow 5-subgroup \mathbf{N}_5 and a unique Sylow 7-subgroup \mathbf{N}_7 . The uniqueness of each of these groups implies that they are normal in \mathbf{G} .

Observe next that $\mathbf{N}_5 \cap \mathbf{N}_7$ is trivial, since only the identity element can have order dividing both $|\mathbf{N}_5|$ and $|\mathbf{N}_7|$. By the Third Isomorphism theorem, we have

$$\mathbf{N}_5\mathbf{N}_7/\mathbf{N}_7 \cong \mathbf{N}_5/\mathbf{N}_5 \cap \mathbf{N}_7 = \mathbf{N}_5$$

Applying Lagrange's theorem, we have

$$\begin{aligned} |\mathbf{N}_5\mathbf{N}_7/\mathbf{N}_7| &= |\mathbf{N}_5| \\ \frac{|\mathbf{N}_5\mathbf{N}_7|}{|\mathbf{N}_7|} &= |\mathbf{N}_5| \\ |\mathbf{N}_5\mathbf{N}_7| &= |\mathbf{N}_5||\mathbf{N}_7| = |\mathbf{G}| \end{aligned}$$

Hence, $\mathbf{G} \cong \mathbf{N}_5 \times \mathbf{N}_7$.

We proceed by showing \mathbf{N}_5 is Abelian. Since \mathbf{N}_5 is of prime power order, it has a nontrivial center $Z(\mathbf{N}_5)$. Furthermore, $Z(\mathbf{N}_5)$ is normal in \mathbf{N}_5 , so $\mathbf{N}_5/Z(\mathbf{N}_5)$ is a group of size 1 or 5. If it is of size 5, then it is cyclic. We claim that this is impossible in general.

Claim 1. *If a group \mathbf{G} properly contains its center, then $\mathbf{G}/Z(\mathbf{G})$ is not cyclic.*

Proof. Suppose, to the contrary, that $\mathbf{G}/Z(\mathbf{G})$ is cyclic generated by $aZ(\mathbf{G})$. We argue that \mathbf{G} is Abelian. Let b and c be elements of \mathbf{G} . We can find integers m and n so that

$$\begin{aligned} bZ(\mathbf{G}) &= a^m Z(\mathbf{G}) \\ cZ(\mathbf{G}) &= a^n Z(\mathbf{G}) \end{aligned}$$

This further implies that we can find elements d and e in $Z(\mathbf{G})$ so that

$$\begin{aligned} b &= a^m d \\ c &= a^n e \end{aligned}$$

Observe that d and e commute freely with any element since they are in the center. Furthermore, powers of a commute with each other. It follows that

$$\begin{aligned} bc &= (a^m d)(a^n e) \\ &= (a^n e)(a^m d) \\ &= cb \end{aligned}$$

Hence, \mathbf{G} is Abelian, so $Z(\mathbf{G}) = \mathbf{G}$, which contradicts our assumption that \mathbf{G} properly contains its center. Therefore, we conclude that $\mathbf{G}/Z(\mathbf{G})$ is not cyclic. \square

Citing the claim above, we conclude that $\mathbf{N}_5/Z(\mathbf{N}_5)$ is of size 1. In other words, \mathbf{N}_5 is Abelian.

Similarly, we can show that \mathbf{N}_7 is Abelian (replace every occurrence of “5” with “7” in the argument for \mathbf{N}_5).

Taken together, we see that $\text{Gal}(E/\mathbb{Q})$ is Abelian, and so is solvable. \square

5 Problem 21

Proposition 5.1. *Let F be a field. The following are equivalent.*

1. F is not algebraically closed, but there is a finite upper bound on the degrees of the irreducible polynomials in $F[x]$.
2. F is a real closed field.

Proof. (1 \Rightarrow 2) We claim first that if there is an upper bound for the degrees of the irreducible polynomials in $F[x]$, then F is perfect. If not, then F has characteristic $p \neq 0$ and some $a \in F$ is not a p^{th} power in F . We have shown that $f(x) = x^{p^t} - c$ is irreducible for every $t \geq 0$, which is a contradiction with the fact that there is a finite upper bound on the degrees of the irreducible polynomials in $F[x]$. Hence, F is perfect. Let K be the algebraic closure of F . Now, we also have that K is separable over F , so the degree of every element of K over F is bounded. Therefore, $[K : F]$ is finite, and so F is real closed by the Artin-Schreier Theorem.

(2 \Rightarrow 1) Let K denote the algebraic closure of F . Since F is real closed, $K = F[\sqrt{-1}]$, and so $[K : F] = 2$. Hence, every irreducible polynomial in $F[x]$ is at most quadratic. \square

6 Problem 22

Let E be the splitting field over \mathbb{Q} of $x^4 - 2$. We determine the lattice of intermediate fields between E and \mathbb{Q} .

Observe first that $x^4 - 2 = (x + \sqrt[4]{2})(x - \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})$, and so $E = \mathbb{Q}[i, \sqrt[4]{2}]$. Now, the elements of the Galois group are determined by their action on the roots of $x^4 - 2$ and, furthermore, their action is restricted to permutations of these roots. Finally, if ϕ is an element of the Galois group $\phi(-\sqrt[4]{2}) = -\phi(\sqrt[4]{2})$ and $\phi(-i) = -\phi(i)$. Hence, we can determine the permutations by sending $\sqrt[4]{2}$ to any of the four roots (which also determines the action on $-\sqrt[4]{2}$) and then sending i to any of the remaining two roots (which also determine the action on $-i$), giving a total of 8 distinct permutations. Define

$$\sigma(x) = -x$$

and

$$\tau(x) = \begin{cases} i & : x = \sqrt[4]{2} \\ -i & : x = i \\ -\sqrt[4]{2} & : x = -i \\ \sqrt[4]{2} & : x = -\sqrt[4]{2} \end{cases}.$$

Computation shows that $\{1, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\}$ are the desired permutations, and so the Galois group is isomorphic to D_8 . We conclude with a presentation of the lattice of subgroups of D_8 (which is well-known), and invoke the Fundamental Theorem of Galois Theory which states that the lattice of subfields of $\mathbb{Q}[i, \sqrt[4]{2}]$ is determined by computing the fixed field of each subgroup of D_8 (generating a lattice of subfields that is “upside-down isomorphic” to the lattice of subgroups).

7 Problem 23

Proposition 7.1. *The field of real numbers has only one ordering that makes it into an ordered field.*

Proof. Any ordering \leq of \mathbb{R} must admit that if $x \leq y$, then $y - x \geq 0$. Since \mathbb{R} is real closed, every positive element of \mathbb{R} is a square. Hence, we can define the relation $x \leq y$ if and only if $y - x = a^2$ for some $a \in \mathbb{R}$. Since the choice of a (if it exists) is unique for each $x, y \in \mathbb{R}$, there can be only one ordering of \mathbb{R} . \square