ALGEBRA HW 11

CLAY SHONKWILER

1

Suppose $k \subset K$ is a separable field extension of degree n.

(a): Show that $K \simeq k[x]/(f(x))$ for some $f(x) \in k[x]$ of degree n.

Proof. By the primitive element theorem, $K = k[\alpha]$ for some $\alpha \in K$. If f is the minimal polynomial of α over k, then $K = k[\alpha] \simeq k[x]/(f(x))$. Then

$$\deg f = [K : k] = n,$$

so we see that $K \simeq k[x]/(f(x))$ where $f(x) \in k[x]$ has degree n. □

(b): Show that $K \otimes_k K \simeq K[y]/(f(y))$ as K-algebras.

Proof. Since $K \simeq k[x]/(f(x))$, we see that

$$K \otimes_k K \simeq k[x]/(f(x)) \otimes_k k[y]/(f(y)) \simeq k[x,y]/(f(x), f(y)).$$

On the other hand,

$$K[y]/(f(y)) \simeq (k[x]/(f(x)))\,[y]/(f(y)) \simeq k[x,y]/(f(x), f(y)),$$

so we see that

$$K \otimes_k K \simeq k[x,y]/(f(x), f(y)) \simeq K[y]/(f(y)).$$

□

(c): Deduce that if K is Galois over k, then $f(y)$ splits over K, and $K \otimes_k K \simeq K^n$ as K-algebras.

Proof. If K is Galois over k, then, since $K \simeq k[y]/(f(y))$, it must be the case that $f(y)$ splits over K (else K would not be normal over k). Hence, $f(y) = \prod_{i=1}^{n}(y-\alpha_i)$ for $\alpha_i \in K$, $i = 1, \ldots, n$. Since $(y-\alpha_i)$ is maximal in $K[y]$ and $(f(x)) = (\prod_{i=1}^{n}(y-\alpha_i)) = (y-\alpha_1)\cdots(y-\alpha_n)$, we know, by the Chinese Remainder Theorem, that

$$K[y]/(f(x)) \simeq K[y]/(y-\alpha_1) \times \cdots \times K[y]/(y-\alpha_n).$$

Now, since $K[y]/(y-\alpha_i) \simeq K$, this implies that $K[y]/(f(x)) \simeq K^n$. Therefore, using the result from (b) above,

$$K \otimes_k K \simeq K[y]/(f(x)) \simeq K^n.$$

□

2

Let R be an ordered field whose squares are the non-negative elements. Suppose that the elements of $R[x]$ satisfy the intermediate value theorem. Let $C = R[x]/(x^2+1)$.

(a): Show that R has characteristic 0, and that every odd degree polynomial over R has a root in R. Deduce that every non-trivial Galois extension of R has even degree.

Proof. Suppose R has characteristic p. Then, since $\leq$ respects addition, $1 \leq 1+1 \leq \ldots \leq p-1$. However, $p-1+1 = 0$, and so we have $0 \leq 1 \leq 1+1 \leq \ldots \leq p-1 \leq 0$, meaning that $0 = 1$, which is impossible. Therefore, it must be the case that R has characteristic 0.

Now, suppose f is an odd degree polynomial over R. Then $f(x) = a_{2n+1}x^{2n+1} + \ldots + a_1 x + a_0$. Suppose $a_{2n+1} \leq 0$. Then, for x sufficiently small, the leading term dominates all other terms so, since $x^{2n+1} \leq 0$ for $x \leq 0$, $f(x_0) \geq 0$ for x_0 sufficiently small. On the other hand, for $x \geq 0$, $x^{2n+1} \geq 0$, so, for x_1 sufficiently large, $f(x_1) \leq 0$. Therefore, since the elements of $R[x]$ (including f) satisfy the intermediate value theorem, $f(x) = 0$ for some $x_0 \leq x \leq x_1$. That is, f has a root in R.

Now, suppose K is a finite extension of R. Then, by the primitive element theorem, there exists $\alpha \in K$ such that $K = R[\alpha]$. In turn, since $R[\alpha] \simeq R[x]/(f(x))$ where $f(x) \in R[x]$ is the minimal polynomial of α over R, we see that $K \simeq R[x]/(f(x))$. Now, since f is irreducible over R, it's clear that $\deg f$ must be even, by the result proved above. However, since $[K : R] = \deg f$, this in turn means that K must have even degree as an extension of R. Since our choice of K was arbitrary, we see that every finite extension of R must be of even degree. $\square$

(b): Show that C is a field, that every element of C is a square of an element of C, and that C has no field extensions of degree 2.

Proof. Since the two roots of x^2+1 in $\bar{R}$ are $\sqrt{-1}$ and $-\sqrt{-1}$ and the squares in R are the non-negative elements, x^2+1 is irreducible, so $C = R[x]/(x^2+1)$ is a field. Now, for any element in $R[x]/(x^2+1)$, we can reduce higher-order terms by $x^2 = -1$, so a generic element in C is of the form $a + bx$ for some $a, b \in R$. If $a = b = 0$, then it's clear that $a + bx = 0 + 0x = (0+0x)^2$. Otherwise, let

$$c = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} \qquad d = \frac{b}{2}\sqrt{\frac{2}{a+\sqrt{a^2+b^2}}}.$$

Then, since $\sqrt{a^2+b^2} \geq |a|$, (where $|a| = a$ if $a \geq 0$ and $|a| = -a$ if $a \leq 0$), so c and d are both in R, and so $c + dx \in C$. Furthermore,

$$\begin{aligned}
(c+dx)^2 &= c^2 - d^2 + 2cdx \\
&= \frac{a+\sqrt{a^2+b^2}}{2} - \frac{b^2}{4}\left(\frac{2}{a+\sqrt{a^2+b^2}}\right) + 2\left(\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}\right)\left(\frac{b}{2}\sqrt{\frac{2}{a+\sqrt{a^2+b^2}}}\right)x \\
&= \frac{(a+\sqrt{a^2+b^2})^2}{2(a+\sqrt{a^2+b^2})} - \frac{b^2}{4}\left(\frac{4}{2(a+\sqrt{a^2+b^2})}\right) + 2\frac{b}{2}\sqrt{\frac{2(a+\sqrt{a^2+b^2})}{2(a+\sqrt{a^2+b^2})}}x \\
&= \frac{a^2+2a\sqrt{a^2+b^2}+a^2+b^2}{2(a+\sqrt{a^2+b^2})} - \frac{b^2}{2(a+\sqrt{a^2+b^2})} + bx \\
&= \frac{2a^2+2a\sqrt{a^2+b^2}}{2(a+\sqrt{a^2+b^2})} + bx \\
&= a + bx.
\end{aligned}$$

Since our choice of $a + bx \in C$ was arbitrary, we see that every element of C is a square of an element of C.

Now, suppose K is a field extension of C of degree 2. Then, since C contains a second root of unity (namely -1), Kummer's Theorem tells us that $K = C[\sqrt{\alpha}]$ for some $\alpha \in C$. However, since, by the above result, $\alpha = \beta^2$ for some $\beta \in C$, we see that $K = C[\sqrt{\alpha}] = C[\beta] = C$, contradicting the supposition that K is an extension of degree 2. Therefore, we see that C has no field extensions of degree 2. □

(c): Show that if $R \subset C \subset L$ are finite field extensions and L is Galois over R with group G, then G is a 2-group.

Proof. Since, by (a), L must be an even extension of R, $\#G$ is divisible by 2, so $\#G = 2^r m$ for some $r \geq 1$ and m relatively prime to 2. Furthermore, G contains a Sylow 2-subgroup H with $\#H = 2^r$. Now, let $K = L^H$, the fixed field of H; then L is Galois over K with Galois group H. Furthermore, since $[L : R] = 2^r m$ and $[L : K] = \#H = 2^r$, $[K : R] = m$, which is relatively prime to 2 and, in particular odd. However, we showed that R has no non-trivial odd degree extensions, so it must be the case that $K = R$ and so $m = 1$. Hence, $G = H$, so G is a 2-group. □

(d): In the situation of (c), show that $L = C$.

Proof. Since L is finite over R, $L = R[\alpha]$ for some $\alpha \in R$. Let f be the minimal polynomial of α over R. Then, since L is Galois over R, f splits over L. Thus, if g is the minimal polynomial of α over C, then $g|f$ and so g splits over L, meaning that L is normal over C. Since C has characteristic 0, L is necessarily separable over C, so we see that L is Galois over C. Since $[L : R] = 2^r$ and $[C : R] = 2$, $[L : C] = 2^{r-1}$, so $\#\text{Gal}(L/C) = 2^{r-1}$. By Cauchy's Theorem, $\text{Gal}(L/C)$ has a subgroup H_1 of order 2. Let $K_1 = L^{H_1}$. Then $[L : K_1] = 2^{r-2}$, so, if $r \geq 2$, $[K_1 : C] = 2$, contradicting the result proved in (b) above. Therefore, we see that $r = 1$, meaning that $[L : K] = 2^{r-1} = 1$, so $L = C$. □

(e): Conclude that C is algebraically closed.

Proof. Suppose K is an algebraic extension of C. Let $\widetilde{K}$ be the algebraic closure of K over C. Then we have $R \subset C \subset \widetilde{K}$ fulfilling the hypotheses of (c), so, by (c) and (d), $\widetilde{K} = C$. Therefore, $K = C$. Since our choice of K was arbitrary, we see that there are no non-trivial algebraic extensions of C, so C is algebraically closed. □

(f): Deduce in particular that the field $\mathbb{C}$ of complex numbers is algebraically closed.

Proof. Since $\mathbb{R}$ is an ordered field, the elements of $\mathbb{R}[x]$ satisfy the intermediate value theorem, and $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$, we see that, by (a)-(e), $\mathbb{C}$ is algebraically closed. □

3

Let p be a prime number, and let $K \subset L$ be a field extension of degree p that is separable but not Galois. Let $\widetilde{L}$ be the Galois closure of L over K. Show that $\widetilde{L}$ does not contain *any* subfield M which is Galois over K of degree p.

Proof. First, note that, by the primitive element theorem, $L = K[\alpha]$ for some $\alpha \in L$ and the minimal polynomial f of α has degree p. Since L is separable, f is separable. $\widetilde{L}$ is obtained from L simply by adjoining all the roots of f and any K-automorphism of $\widetilde{L}$ permutes the roots of f. Since there are p roots of f (since f is separable), we see that $\text{Gal}(\widetilde{L}/K)$ is the subgroup of S_p consisting of the possible permutations of the roots of f. In particular, this means that $\#\text{Gal}(\widetilde{L}/K)|p!$.

Now, suppose $\widetilde{M}$ contains a subfield M which is Galois over K of degree p. Then $\text{Gal}(M/K) = C_p$. Hence, LM is Galois over L, and $\text{Gal}(LM/L)$ is a subgroup of C_p. Since the only such subgroups are the trivial group and C_p itself, we see that either $\text{Gal}(LM/L) = 1$ or $\text{Gal}(LM/L) = C_p$. In the first case, this implies that $LM = L$, which is impossible, since this implies $M = L$ and L is not Galois over K. On the other hand, if $\text{Gal}(LM/L) = C_p$, then we have that $L \cap M = K$, which in turn implies that $[LM : K] = [L : K][M : K] = p^2$. On the other hand,

$$p^2 = [LM : K] \mid [\widetilde{L} : K] = \#\text{Gal}(\widetilde{L}/K) = p!.$$

This implies that $p|(p-1)!$, which is impossible since p is prime. Therefore, we conclude that, in fact, there is no such M, so $\widetilde{L}$ does not contain any subfield M which is Galois over K of degree p. $\square$

4

(a): Prove that any polynomial $f(x) \in \mathbb{Q}[x]$ of degree < 5 is solvable by radicals.

Proof. Clearly, it suffices to show that any irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree < 5 is solvable by radicals. To that end, let $f(x) \in \mathbb{Q}[x]$ be irreducible and of degree $n < 5$; we may as well also assume f is monic. Let L be the splitting field of f and let $a_1, \ldots, a_n$ be the roots of f in $\overline{\mathbb{Q}}$. Then any $\mathbb{Q}$-automorphism of L consists simply in permuting the a_i, so we see that $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of S_n. Since any subgroup of a solvable group is solvable and an irreducible polynomial in $\mathbb{Q}[x]$ is solvable by radicals if and only if the Galois group of its splitting field is solvable, we see that f is solvable if and only if S_n is solvable.

Now, $S_1 = 1$ and $S_2 = 2$ are trivially solvable. Also, as a subgroup of S_3, $\langle(123)\rangle \simeq C_3$ is of index 2 in S_3 and is, therefore, normal. Hence, we have the composition series

$$1 \lhd \langle(123)\rangle \lhd S_3,$$

the the quotients are C_3 and C_2 from left to right, so we see that S_3 is solvable.

Finally, A_4 is a subgroup of index 2 in S_4, so $A_4 \lhd S_4$. Now, let $G = \{1, (12)(34), (13)(24), (14)(23)\}$. Then, as we've seen, $G \lhd S_4$, so $G \lhd A_4$. Furthermore, since $\#A_4 = 12$ and $\#G = 4$, it must be the case that $A_4/G \simeq C_3$. Since $A_4 \simeq C_2 \times C_2$, we see that we have the following composition series for S_4:

$$1 \lhd C_2 \lhd G \lhd A_4 \lhd S_4,$$

which has quotients C_2, C_2, C_3, C_2 from left to right, so we see that S_4 is solvable. Since $1, 2, 3, 4$ are the only possibilities for $n < 5$, we see that f must be solvable by radicals. Since our choice of f was arbitrary, we see that any irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree < 5 is solvable by radicals. $\square$

(b): Find an $\alpha \in \overline{\mathbb{Q}}$ whose irreducible polynomial over $\mathbb{Q}$ has degree 5, and is solvable by radicals.

Example: Let $\alpha = \zeta_{11} + \zeta_{11}^{-1}$. Then, by the result proved in PS10#2(d), $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$ with Galois group C_5. Since $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f(x))$ where f is the irreducible polynomial of α over $\mathbb{Q}$, we see that $\deg f = \#\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = 5$. Furthermore, since C_5 is a solvable group (composition series: $1 \lhd C_5$), we see that $f(x)$ is solvable by radicals.

♣

5

(a): Let p be a prime number, and let G be a subgroup of S_p. Suppose G contains a transposition and a p-cycle. Show that $G = S_p$.

Proof. Clearly, if $p = 2$, then $S_2 = C_2$, so the only non-identity element is the unique 2-cycle, so G containing a 2-cycle means $G = S_2$. Hence, suppose p is an odd prime and suppose $(1a_1 \dots a_{p-1})$ is the p-cycle in G (we can always write a p-cycle in this form) and (b_1b_2) is the transposition in G. Then $b_1 = a_i$ for some i and $b_2 = a_j$ for some j. Then $(1a_1 \dots a_{p-1})^{-1} = (1a_{p-1} \dots a_1)$ and

$$(1a_1 \dots a_{p-1})(b_1b_2)(1a_{p-1} \dots a_1) = (1a_2 \dots a_p)(a_ia_j)(1a_p \dots a_2) = (a_{i+1}a_{j+1}) \in G,$$

where we figure $i + 1$ and $j + 1$ module p with $a_0 = 1$. Now, $(1a_1 \dots a_{p-1})^2 = (1a_2a_4 \dots a_{p-1}a_1a_3 \dots a_{p-2})$. Then

$$(1a_2a_4 \dots a_{p-1}a_1a_3 \dots a_{p-2})(a_ia_j)(1a_{p-2}a_{p-4} \dots a_1a_{p-1}a_{p-3} \dots a_2) = (a_{i+2}a_{j+2}) \in G,$$

again figuring $i + 2$ and $j + 2$ modulo p. Iterating this process, we see that

$$(a_ia_j), (a_{i+1}a_{j+1}), \dots, (a_{i+(p-1)}a_{j+(p-1)}) \in G,$$

where we figure the $i+k$ and $j+k$ modulo p. Now, $a_{i+(p-i)} = a_0 = 1$, so $(1a_{j+(p-i)}) \in G$. Now, $j + (p - i) = i + k_1$ for some k_1, so $(a_{i+k_1}a_{j+(p-i)}) \in G$, and so

$$(a_{i+k_1}a_{j+(p-i)})(1a_{j+(p-i)})(a_{i+k_1}a_{j+(p-i)}) = (1a_{i+k_1}) \in G.$$

In turn, $i + k_1 = j + k_2$ for some k_2, so $(a_{i+k_2}a_{i+k_1}) \in G$ and so

$$(a_{i+k_2}a_{i+k_1})(1a_{i+k_1})(a_{i+k_2}a_{i+k_1}) = (1a_{i+k_2}) \in G.$$

Iterating this process, we see that

$$(12), (13), \dots, (1(p-1)) \in G.$$

Now, if $(ab) \in S_p$ is a transposition, then

$$(1a)(1b)(1a) = (ab) \in G.$$

Therefore, we see that all transpositions are in G; since the transpositions generate S_p, this, in turn, implies that $S_p \subset G$. Since $G \subset S_p$, we see that $G = S_p$. □

(b): Suppose that $f(x) \in K[x]$ is a separable irreducible polynomial of degree p, and let G be the Galois group of f over K. Show that G is a subgroup of S_p; that p divides the order of G; and that G contains a p-cycle.

Proof. Let L be the splitting field of f over K. Then L is Galois over K since f is separable. Now, if $a_1, \dots, a_p$ are the p distinct roots of f (again, f has exactly p distinct roots since it is separable), then any K-automorphism of L is a permutation of the a_i, so we see that $G = \mathrm{Gal}(L/K) \subset S_p$. Now, $K[a_1] \subset L$ is a field extension. Since f is satisfied by a_1, the minimal polynomial of a_1 over K must divide f and, hence, since f is irreducible, the minimal polynomial must also be of degree p. Hence, $[K[a_1] : K] = p$. Since $L = K[a_1, \dots, a_p]$,

$$\#G = [L : K] = [K[a_1] : K][K[a_1, a_2] : K[a_1]] \cdots [L : k[a_1, \dots, a_{p-1}]],$$

so, since $[K[a_1] : K] = p$, we see that p divides the order of G. Since p divides the order of G, G must contain an element of order p, by Cauchy's Theorem. Now, the only elements of S_p of order p are the p-cycles, so we see that G contains a p-cycle. □

(c): Suppose that $f(x) \in \mathbb{Q}[x]$ is irreducible of degree p and that exactly two of its roots do not lie in $\mathbb{R}$. Let G be the Galois group of f. Show that G contains a transposition, and deduce that G is isomorphic to S_p.

Proof. Let L be the splitting field of f. Let $a + bi$ and $a - bi$ be the two non-real roots of f (we know they are of this form, since any non-real roots must come in conjugate pairs). Let $\phi : L \to L$ be the map such that $\phi(r) = r$ for all real $r \in L$ and $\phi(a+bi) = a-bi$. Since $L = \mathbb{Q}[a_1, \dots, a_p]$ where the a_i are the roots of f, ϕ in fact defines a $\mathbb{Q}$-automorphism of L, since it simply fixes all the a_i except $a + bi$ and $a - bi$, which it swaps. Hence, $\phi \in G$. Since $\phi \circ \phi = id$, ϕ has order 2 and so corresponds to a transposition.

Therefore, G contains a transposition and, by our work in (b) above, a p-cycle. Therefore, by the result proved in (a), $G = S_p$. □

(d): Deduce that $3x^5 - 6x - 2$ is not solvable by radicals.

Proof. First, note that 2 does not divide 3, 2 does divide -6 and -2, but 4 does not divide -2, so, by Eisenstein's Criterion, $3x^5 - 6x - 2$ is irreducible. Let $f(x) = 3x^5 - 6x - 2$. Then

$$f'(x) = 15x^4 - 6.$$

Hence, the only real critical points of f are $\sqrt[4]{\frac{6}{15}}$ and $-\sqrt[4]{\frac{6}{15}}$, so f has at most 2 local extrema and, therefore, $f(x) = 0$ for at most 3 real values of x. On the other hand, $f(-2) = -86$, $f(-1) = 1$, $f(0) = -2$ and $f(2) = 88$, so, by the intermediate value theorem, f has at least 3 real roots: between -2 and -1, between -1 and 0, and between 0 and 2. Therefore, f has exactly 3 real roots and, hence, exactly two roots that do not lie in $\mathbb{R}$. Hence, if G is the Galois group of f over $\mathbb{Q}$, G contains a p-cycle by (b) and a transposition by (c), so $G = S_5$, by (a). Since S_5 is not solvable, we see that $f(x) = 3x^5 - 6x - 2$ is not solvable by radicals. $\square$

6

For which positive integers n is it possible, with straightedge and compass, to divide *any* given angle into n equal parts? Prove your assertions.

Answer: We claim that we can n-sect an angle if and only if $n = 2^r$ for some $r \in \mathbb{N}$. Clearly, by iteratively bisecting an angle, we can 2^r-sect an angle for all $r \in \mathbb{N}$. On the other hand, note first that if we can mn-sect an angle for some $m, n \in \mathbb{N}$, then, by taking m of the mn-sections that are adjacent to eachother, we have effectively n-sected the angle. Therefore, it suffices to show that we cannot p-sect an angle for any odd prime p.

Now, suppose p is an odd prime. Note that, as we saw in class, we can construct an angle of $\frac{2\pi}{n}$ only if we can construct a regular n-gon. Since we can only construct a regular n-gon if $n = 2^r p_1 \cdots p_k$ for p_i Fermat primes and $2 < p_1 < \ldots < p_k$, it's clear that if p is not a Fermat prime, then we cannot construct a regular $6p$-gon, and so we cannot construct an angle of $\frac{2\pi}{6p}$ radians. On the other hand, we can construct the angle $\frac{\pi}{3} = \frac{2\pi}{6}$, so this implies that we cannot p-sect the 60° angle. On the other hand, suppose p is a Fermat prime. Then it is possible that we can construct the angle of $\frac{2\pi}{6p}$ radians. If not, then, again, we cannot p-sect the angle $\frac{\pi}{3}$. If so, then we claim that we cannot p-sect the constructible angle $\frac{2\pi}{6p}$. To see why, simply note that $6p^2$ is not of the form $2^r p_1 \cdots p_k$ where the p_i are Fermat primes and $2 < p_1 < \ldots < p_k$, since we have $6p^2 = 2 \cdot 3 \cdot p \cdot p$. 3 and p are Fermat primes, but $p \not< p$. Therefore, since we cannot construct the regular $6p^2$-gon, we cannot construct the angle $\frac{2\pi}{6p^2}$, which means we cannot p-sect the constructible angle $\frac{2\pi}{6p}$.

Having examined all cases, we see that we cannot p-sect the angle for any odd prime p, and so we cannot n-sect an angle unless $n = 2^r$ for some $r \in \mathbb{N}$.

♣

DRL 3E3A, University of Pennsylvania
E-mail address: shonkwil@math.upenn.edu