

MATH 123: ABSTRACT ALGEBRA II
SOLUTION SET # 9

GREGG MUSIKER

1. CHAPTER 13, SECTION 3

Problem 1 Let F be a field, and let α be an element which generates a field extension of F of degree 5. Then, α^2 generates the same extension.

Since $\alpha^2 \in F(\alpha)$, this implies $F \subset F(\alpha^2) \subset F(\alpha)$. By multiplicativity of degree, $5 = [F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$.

Since α is a root of $f(x) = x^2 - \alpha^2$, where $f(x) \in F(\alpha^2)[x]$, $[F(\alpha) : F(\alpha^2)] = 1$ or 2 depending on whether or not f is irreducible in $F(\alpha^2)[x]$. But $2 \nmid 5$, so $[F(\alpha) : F(\alpha^2)] = 1$ which implies f is reducible and $\alpha \in F(\alpha^2)$ which implies $F(\alpha) \subset F(\alpha^2)$, and by mutual inclusion, $F(\alpha) = F(\alpha^2)$.

NOTES: if α generated an extension of degree n where n was any odd number, the same proof would imply that the two extensions $F(\alpha)$ and $F(\alpha^2)$ were identical. Also since 5 is a prime, Corollary 13.3.7 of Artin implies that $K = F(\alpha)$ is the same as $F(\beta)$ for $\beta = \alpha^2$.

Problem 6 Let a be a positive rational number which is not a square in \mathbb{Q} . Then $\sqrt[4]{a}$ has degree 4 over \mathbb{Q} .

Three methods for doing this problem:

1) Clearly, $b = \sqrt[4]{a}$ is a root of $f(x) = x^4 - a$. Thus, it suffices to show that $f(x)$ is irreducible. First, assume that $f(x)$ has a linear factor. This would imply that the factor is $(x - b\zeta_4)$ where ζ_4 is a fourth root of unity, namely, $1, i, -1, \text{ or } -i$. But this implies $b\zeta_4 \in \mathbb{Q}$ but $b^2 = \pm\sqrt{a}$ is not even in \mathbb{Q} thus $f(x)$ has no linear factor. Next, assume that $f(x)$ breaks into two quadratics. Since $f(x)$ has no coefficients for x, x^2 and x^3 , it must be the case $f(x) = (x^2 + \sqrt{a})(x^2 - \sqrt{a})$ but again $\sqrt{a} \notin \mathbb{Q}$ so this is impossible. Thus $f(x)$ is irreducible, and $[\mathbb{Q}(b) : \mathbb{Q}] = 4$.

2) We build the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{a}) \subset \mathbb{Q}(b)$. Since b is a root of $f(x)$, $[\mathbb{Q}(b) : \mathbb{Q}] \leq 4$. By assumption $\sqrt{a} \notin \mathbb{Q}$ which means that $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2$ and by multiplicativity of degree, this implies $2 \mid [\mathbb{Q}(b) : \mathbb{Q}]$. We conclude that $[\mathbb{Q}(b) : \mathbb{Q}] = 4$ and not $[\mathbb{Q}(b) : \mathbb{Q}] = 2$ by considering $f(x) = (x^2 + \sqrt{a})(x^2 - \sqrt{a})$ but again $\sqrt{a} \notin \mathbb{Q}$ so this is impossible.

3) Let $a = m/n$ where m and n are relatively prime. Thus if prime $p \mid m$ then $p \nmid n$. since a is not a square in \mathbb{Q} , this implies there exists some prime factor p of either m or n s.t. $p \mid m$ but $p^2 \nmid m$. (NOTE: This does not imply that m or n is square-free, only that at least one of the prime factors has an exponent of one.) Assume $p \mid m$ but $p^2 \nmid m$. Then $g(x) = nx^4 - m$ is irreducible over $\mathbb{Z}[x]$ by Eisenstein's criterion and consequently, $f(x) = \frac{1}{n}g(x)$ is irreducible in $\mathbb{Q}[x]$. If m is a square, then n is

not, and consider $\alpha = \frac{1}{a}$. Then $x^4 - \alpha$ is irreducible, which means that $F = \mathbb{Q}(1/b)$ is a degree 4 extension over \mathbb{Q} and since F is a field, $F = \mathbb{Q}(b)$ as well.

Problem 7 *Decide whether i is in the field F .*

a) $F = \mathbb{Q}(\sqrt{-2})$. If $i \in F$ then $\alpha = i\sqrt{-2} \in F$. But $\alpha^2 - 2 = 0$. Which implies $\alpha = \pm\sqrt{2}$, and thus $\sqrt{2} = a + b\sqrt{-2} \in F$ for some $a, b \in \mathbb{Q}$. But then

$$a^2 + 2ab\sqrt{-2} - 2b^2 = 2 \implies \sqrt{-2} = \frac{a^2 - 2b^2 - 2}{-2ab}$$

but $\sqrt{-2}$ is not rational. Thus $i \notin F$.

b) $F = \mathbb{Q}(\sqrt[4]{-2})$. By Problem 6, $[F : \mathbb{Q}] = 4$. $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. But $i \in F \implies F = F(i)$ and $4 = [F : \mathbb{Q}] = [F(i) : \mathbb{Q}] = [F(i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2[F(i) : \mathbb{Q}(i)]$ which implies $[F(i) : \mathbb{Q}(i)] = 2$. Since $\sqrt[4]{-8} \in F$ there exists $a, b \in \mathbb{Q}(i)$ such that $a + b\sqrt[4]{-2} = \sqrt[4]{-8}$.

$$a^2 + 2ab\sqrt[4]{-2} - \sqrt{-2}b^2 = 2\sqrt{-2}.$$

Reorganizing these terms, we find that $i \in F$ implies $\sqrt[4]{-2} \in \mathbb{Q}(i, \sqrt{-2})$, but squaring both sides of $\sqrt[4]{-2} = a + b\sqrt{2} + c\sqrt{-2} + di$ we get $\sqrt[4]{-2} \in \mathbb{Q}(\sqrt{2})$ which we know is impossible since $[F : \mathbb{Q}] = 4$. Consequently, $i \notin F$.

c) $F = \mathbb{Q}(\alpha)$ where $\alpha^3 + \alpha + 1 = 0$. Any factorization of this polynomial would involve a linear term so by the rational root (for ± 1) this polynomial is irreducible and $[F : \mathbb{Q}] = 3$. If $i \in F$, $3 = [F : \mathbb{Q}] = [F(i) : \mathbb{Q}] = [F(i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2[F(i) : \mathbb{Q}(i)]$. But $2 \nmid 3$ so that is impossible, and $i \notin F$. (NOTE: Even though this cubic has a real root which and if $\alpha \in \mathbb{R}$ then $i \notin F$, the cubic also has complex roots as well, and we don't get to choose α .)

Problem 10 *Let α, β be complex numbers. If $\alpha + \beta$ and $\alpha\beta$ are both algebraic, then show α and β are also algebraic.*

It is given that $\mathbb{Q} \subset \mathbb{Q}(\alpha + \beta, \alpha\beta)$ is algebraic. We will show that $\mathbb{Q}(\alpha + \beta, \alpha\beta) \subset \mathbb{Q}(\alpha, \beta)$ is algebraic hence $\mathbb{Q} \subset \mathbb{Q}(\alpha, \beta)$ is algebraic. Consider $f(x) = x^2 - (\alpha + \beta)x + \alpha\beta \in \mathbb{Q}(\alpha + \beta, \alpha\beta)[x]$. This clearly has both α and β in roots, enough said.

2. CHAPTER 13, SECTION 4

Problem 1 *Write $\cos 15^\circ$ in terms of square roots.*

By the half-angle formula from your favorite trigonometry class, $\cos^2 15^\circ = \frac{1 + \cos 30^\circ}{2}$ and $\cos 30^\circ = \frac{\sqrt{3}}{2}$. From $\cos 15^\circ > 0$ we conclude $\cos 15^\circ = \sqrt{\frac{\sqrt{3} + 2}{4}}$. We could simply this further into $\frac{\sqrt{6} + \sqrt{2}}{4}$.

Problem 2 *Show that the regular pentagon can be constructed.*

a) *Using Field Theory* One can construct an angle θ as long as one can construct $\cos \theta$. So it suffices to construct $x = \cos \theta$ where $\theta = 72^\circ = 360^\circ/5$. This can be done via similar triangles where one arrives at the equation

$$\frac{x}{1} = \frac{1}{x - 1}$$

and thus x satisfies an irreducible quadratic equation hence $[\mathbb{Q}(x) : \mathbb{Q}]$ is 2. ($x = \frac{\sqrt{5}-1}{4}$) Additionally, one can use the fact that $5\theta = 360^\circ$ to conclude $\cos \theta = \cos 4\theta$, $\cos 2\theta = \cos 3\theta$ and factor

$$x^5 + x^4 + x^3 + x^2 + x + 1$$

into a product of quadratic and linear factors. Lastly, $5 = 2^n + 1$ so according to Gauss, the regular 5-gon is constructible and a similar argument involving the Euler phi function holds.

b) *Using an Explicit Construction* I am going to spare you all my drawings since all of you had this or something very close. If you have a specific question about this, feel free to ask.

Problem 5 *Is it possible to construct a square that has the same area as a given triangle?*

Yes. Pick a base (one of the sides) and construct the associated perpendicular bisector. You know can construct bh where b is the length of the base, and h is the length of the height. Thus you can construct a segment of length $\sqrt{bh/2}$. Thus create a square using parallels and perpendicular lines whose side lengths are all $\sqrt{bh/2}$. The area of the square and the triangle will both be $bh/2$.

Problem 10 If a prime integer p has the form $2^r + 1$, then it actually has the form $2^{2^k} + 1$.

Let $r = 2^k s$ where s is odd. Then the polynomial $x^r + 1 = y^s + 1$ where $y = x^{2^k}$. Since s is odd, -1 is a root of $y^s + 1$ and $y^s + 1 = (y + 1)(\sum_{i=0}^{s-1} (-y)^i)$. If $s > 1$ and $y \geq 4$ then since $(-y)^{s-1} \geq 4$ will dominate all the lower terms of the sum, $p = y^s + 1$ factors into non-units, this contradicts the primality of p . Note that as long as $k \geq 1$, $y \geq 4$ for $x = 2$. Thus $s = 1$ and $r = 2^k$.

There is another way that totally bypasses field theory and uses group theory¹. Since $2^r \equiv -1 \pmod{p}$, the order of 2 is $2r$ in $\mathbb{Z}/p\mathbb{Z}^\times$. Thus by Lagrange's Theorem, $2r | p - 1$, the order of the group. However, $2r | p - 1 = 2^r$ implies that the only prime factors of r must be 2, hence $r = 2^k$ for some k .

3. CHAPTER 13, SECTION 5

Problem 2 *Let $f(x) = x^p - x \in F[x]$ and p is a prime. For what fields F and primes p will $f(x)$ have a multiple root?*

By Prop 15.5.6, α is a multiple root of $f(x)$ iff $f(\alpha) = 0$ and $f'(\alpha) = 0$ where $f'(x)$ is the formal derivative of $f(x)$. In this case, $f'(x) = px^{p-1} - 1$. Assume

$$\alpha^p - \alpha = 0 \text{ and}$$

$$p\alpha^{p-1} - 1 = 0.$$

Let $\beta = \alpha^{p-1}$. $\beta = \frac{1}{p}$ in F and $\alpha(\beta - 1) = 0$ in F . $0^{p-1} \neq \frac{1}{p}$ thus $\alpha = 0$ is not a multiple root. Since F is a field, it is an integral domain and we might have there is another α that is a multiple root where $\frac{1}{p} = \beta = 1$ in F . This will occur if and only if $p - 1 \equiv 0$ in F which occurs if and only if $\text{char}(F)$ divides $p - 1$. $\text{char}(F)$

¹Thanks to Noam Zeilberger.

is always a prime or zero. If $\text{char} = 0$, this will be impossible, and if $p = 2$, no such field exists with $\text{char}(F) = 1$. *However, if $p \geq 3$, as long as $\text{char}(F)$ divides $p - 1$, then $f(x)$ has a multiple root.* (NOTE: F need not be a finite field, consider $\mathbb{Z}/2\mathbb{Z}(t)$ with char equal to 2.)

Problem 4 *Let $\alpha_1, \dots, \alpha_n$ be the n roots of a degree n polynomial $f(x)$ in $F[x]$. Then what is the best upper bound for $[F(\alpha_1, \dots, \alpha_n) : F]$?*

The best upper bound is $n!$ for the following reasoning:

First, assume that $f(x)$ is irreducible. Then $[F(\alpha_1) : F] = n$. If $f(x)$ were reducible then α_1 would be the root of an irreducible polynomial with degree $< n$ and thus $[F(\alpha_1) : F] = n$. Let $f(x) = (x - \alpha_1)g(x)$. $g(x)$ will have degree $n - 1$. By the same argument, $[F(\alpha_1, \alpha_2) : F(\alpha_1)] \leq n - 1$ where the bound is achieved if $g(x)$ is irreducible.² By continuing this logic inductively, and use the multiplicativity of degree extensions we get an upper bound of $n!$. (NOTE: This field $F(\alpha_1, \dots, \alpha_n)$ is very important in field theory, it is known as the *splitting field* for the polynomial $f(x)$.)

²We also have to insure that α_2 is a root of $g(x)$, i.e. that $\alpha_2 \neq \alpha_1$. Over any extension of \mathbb{Q} , an irreducible polynomial is separable, i.e. has no multiple roots. But over fields of positive characteristic, irreducible does not imply separable. However, there is still plenty of irreducible separable polynomials to use to achieve the upper bound. This is a subtle point which is why I included it only in a footnote.