

MATH113 (BRIEF) SOLUTIONS: HOMEWORK 8

- (1) Suppose we have a tower of field extensions $L \subset K \subset F$, and suppose that F is algebraic over K , and K is algebraic over L . Prove that F is algebraic over L .

Solution: Suppose $\alpha \in F$. Then by algebraicity of F over K , there is a minimal polynomial $p = a_0 + a_1x + \dots + a_mx^m$, with coefficients $a_i \in K$ such that $p(\alpha) = 0$. But each $a_i \in K$ is algebraic over L , and in particular (since extension by a single algebraic element is a finite extension) we have the tower of extensions:

$$L \subset L(a_1) \subset L(a_1, a_2) \subset \dots \subset L(a_1)(a_2) \dots (a_m) \subset L(a_1, \dots, a_m)(\alpha)$$

Each step in the tower above is of finite degree: the first m of them because the a_i 's are algebraic over L , and the last step because α is algebraic over $L(a_1, \dots, a_m)$ (it satisfies p). Therefore, the top field in the tower is a finite extension of L - in particular, it's an algebraic extension, so α is algebraic over L . Since every $\alpha \in F$ is algebraic over L , F is algebraic over L .

- (2) §6.2 #4 Construct a field K with nine elements, and find a cyclic generator of K^\times .

Solution: The polynomial $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$, since it has no roots in \mathbb{F}_3 , and it has degree ≤ 3 . So, as we have seen a few times in class, the quotient $K = \mathbb{F}_3[x]/\langle x^2 + 1 \rangle$ is a field with nine elements. **I did some scratch-work to figure out that:** The element $x + 1 + \langle x^2 + 1 \rangle$ in K is an element of order $8 = |K^\times|$. Here are the calculations:

$$\begin{aligned} (x + 1 + \langle x^2 + 1 \rangle) &= &= x + 1 + \langle x^2 + 1 \rangle \\ (x + 1 + \langle x^2 + 1 \rangle)^2 &= x^2 + 2x + 1 + \langle x^2 + 1 \rangle &= 2x + \langle x^2 + 1 \rangle \\ (x + 1 + \langle x^2 + 1 \rangle)^3 &= 2x^2 + 2x + \langle x^2 + 1 \rangle &= 2x + 1 + \langle x^2 + 1 \rangle \\ (x + 1 + \langle x^2 + 1 \rangle)^4 &= 2x^2 + 3x + 1 + \langle x^2 + 1 \rangle &= 2 + \langle x^2 + 1 \rangle \\ (x + 1 + \langle x^2 + 1 \rangle)^5 &= &= 2x + 2 + \langle x^2 + 1 \rangle \\ (x + 1 + \langle x^2 + 1 \rangle)^6 &= 2x^2 + x + 2 + \langle x^2 + 1 \rangle &= x + \langle x^2 + 1 \rangle \\ (x + 1 + \langle x^2 + 1 \rangle)^7 &= x^2 + x + \langle x^2 + 1 \rangle &= x + 2 + \langle x^2 + 1 \rangle \\ (x + 1 + \langle x^2 + 1 \rangle)^8 &= x^2 + 3x + 2 + \langle x^2 + 1 \rangle &= 1 + \langle x^2 + 1 \rangle \end{aligned}$$

A few notes on this question. (1) We calculate the powers by successively multiplying the representatives by $x + 1$, and then reducing in two ways: first remembering that all the numbers are mod 3, and second remembering that we are working mod $x^2 + 1$ (2) Notice that in the rightmost column, we have all the degree ≤ 2 polynomials over \mathbb{F}_3 (except 0). (3) I could have stopped calculating after I showed that the fourth power was not $1 + \langle x^2 + 1 \rangle$. Why?

- (3) §6.2 #6 Determine all the finite subgroups of \mathbb{C}^\times .

Solution: Briefly, Theorem 6.2.3 in Herstein tells us that such subgroups are cyclic. So we can equivalently ask "What are the elements of finite order in \mathbb{C}^\times ?" **Every cyclic subgroup has a generator, and if the subgroup is finite, then the generator must have finite order!** The elements of finite order are precisely those elements a with the property that $a^n = 1$ for some positive integer n - namely, they are the roots of the polynomials $x^n - 1$. A complex number $z = re^{i\theta}$ has $z^n = 1$ if and only if $r = 1$ (there is only one positive real (radius) whose n th power is 1) and $n\theta = 2k\pi$. **Notice here that any multiple of 2π works o.k. on the right side, since in polar form for a complex number, we only care about the angle up to multiples of 2π ; any angle which is a multiple of 2π gives us complex numbers on the positive x -axis.** Therefore, the generators

of the subgroups we are interested in are all the numbers $e^{i2\pi/n}$. The complete list of finite subgroups of \mathbb{C} is $\{\langle e^{2\pi i/n} \rangle\}_{n \in \mathbb{N}}$, where the pointy braces mean “multiplicative subgroup generated by”. The above was about what I was expecting you to get, but it would be really great to also observe the following: It seems like we might also need some other generators, say $e^{i2k\pi/n}$ for $(k, n) = 1$. But actually we don't need to include these numbers in our list: Notice that $e^{i2k\pi/n} \in \langle e^{2\pi i/n} \rangle$, and if $(k, n) = 1$, then there are integers a, b with $ak + bn = 1$ so $e^{2i\pi/n} = e^{2(ak+bn)\pi/n} = (e^{i2k\pi/n})^a \in \langle e^{i2k\pi/n} \rangle$: this is enough to show that $\langle e^{i2k\pi/n} \rangle = \langle e^{2\pi i/n} \rangle$, so using $e^{i2k\pi/n}$ as one of our generators would be repetitive. The point of the problem was not to make you fuss around with complex numbers, but just to think a little about the theorem 6.2.3. So don't worry so much about rules for multiplying complex numbers etc. Even if this is not familiar, there are many more important things to prepare for.

- (4) In this problem, we correct a mistake from class. Let F be a field, and let α and β have minimal polynomials p_α and p_β , in $F[x]$, respectively. It is **NOT TRUE** that $F(\alpha) \simeq F(\beta)$ if and only if $p_\alpha = p_\beta$.

- (a) Show that over \mathbb{Q} , the algebraic numbers $\sqrt{3}$ and $\sqrt{3} + 1$ have different minimal polynomials, but generate the same extension of \mathbb{Q} .

Solution: $\sqrt{3}$ satisfies $x^2 - 3$, which is 3-Eisenstein, and hence irreducible. $\sqrt{3} + 1$ satisfies $(x - 1)^2 - 3 = x^2 - 2x - 2$, which is 2-Eisenstein, and hence irreducible. So they satisfy different irreducible polynomials. On the other hand, as subrings of the real numbers, these two things are the same, as we can see: $\sqrt{3} + 1 \in \mathbb{Q}(\sqrt{3})$ (by closure under addition). And $\sqrt{3} = (\sqrt{3} + 1) - 1 \in \mathbb{Q}(\sqrt{3} + 1)$, again by closure under addition. Since the generator from each extension is contained in the other, the two extensions are the same (as subrings of \mathbb{R}). So they are the same extension of \mathbb{Q} .

- (b) Show that $f = x^3 + x^2 + 1$ and $g = x^3 + x + 1$ are irreducible over \mathbb{F}_2 . If α is a root of f , and β is a root of g , show that $\mathbb{F}_2(\alpha) \simeq \mathbb{F}_2(\beta)$, even though α and β have different minimal polynomials.

Solution: By the same argument that we have given a few times in class and on HWs, both of these extensions are degree 3 extensions of \mathbb{F}_2 , hence, both of these are fields with $2^3 = 8$ elements. By the basic theorem from finite fields, that means that these two fields are isomorphic as extensions of \mathbb{F}_2 . But α and β clearly have different irreducible polynomials - the ones in the question are irreducible by the usual “check for roots”, since they have degree ≤ 3 , and have no roots (check! I'm skipping over this part).

- (c) Here's a **correct statement**: Let F be a field. Let α and β be algebraic over F with minimal polynomials p_α and p_β . Show that $p_\alpha = p_\beta$ if and only if there is an isomorphism $\phi : F(\alpha) \rightarrow F(\beta)$ with $\phi(\alpha) = \beta$ and $\phi(a) = a$ for all $a \in F$.

Solution: We'll prove this “if and only if” in two steps. Assume that there is an isomorphism $\phi : F(\alpha) \rightarrow F(\beta)$ with $\phi(a) = a$ for all $a \in F$, and $\phi(\alpha) = \beta$. Let $p_\alpha = a_0 + a_1x + \dots + a_nx^n$. We know in $F(\alpha)$ we have the equation $0 = p_\alpha(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n$. And applying ϕ , we get in $F(\beta)$ the equation $0 = a_0 + a_1(\beta) + \dots + a_n\beta^n$. All we used to get this was the properties of ϕ - namely, it is a group homomorphism, so $\phi(0) = 0$, and it fixes all the elements a_i if F , and sends α to β . Notice that we have shown that β satisfies the minimal polynomial for α : so $p_\beta \mid p_\alpha$. By the same argument, we can show that $p_\alpha \mid p_\beta$, so they must be equal. Now for the other direction. Assume $p_\alpha = p_\beta$. Then by

the theorem about “adjoining abstract roots”, we know that

$$F(\alpha) = F[x]/\langle p_\alpha(x) \rangle = F[x]/\langle p_\beta(x) \rangle = F(\beta)$$

Furthermore, the isomorphism $F[x]/\langle p_\alpha(x) \rangle$ was constructed by looking at the ring homomorphism $ev_\alpha : F[x] \rightarrow F[\alpha]$, and applying the First Homomorphism Theorem. In particular, x gets sent to α . Similarly for β . So analyzing the equation above, we see that the isomorphism actually fixes elements of F and maps α to β .

(5) Let $q = p^n$ with p prime and $n \geq 1$. In this problem we find the subfields of \mathbb{F}_q .

(a) Show that if $a|b$ then $x^a - 1 | x^b - 1$ in $\mathbb{Z}[x]$

Solution: The hint was to consider the equality

$$y^n - 1 = (y - 1)(y^{n-1} + y^{n-2} + \dots + y + 1)$$

Letting $a = nb$, and making the substitution $y = x^a$ in the given equality, we get the formula

$$[*] \quad x^b - 1 = x^{na} - 1 = (x^a - 1)(x^{(n-1)a} + x^{(n-2)a} + \dots + x^{2a} + x^a + 1)$$

(b) Let $q' = p^m$ with $m|n$. Show that $q' - 1 | q - 1$.

Solution: This follows immediately from (a) by taking $x = p$, $a = m$, $b = n$.

(c) Show $x^{q'} - x$ divides $x^q - x$, and conclude that \mathbb{F}_q contains $\mathbb{F}_{q'}$ as a subfield.

Solution: $x^q - x = x(x^{q-1} - 1)$ and similarly for $x^{q'} - x = x(x^{q'-1} - 1)$. But from part (b), $q' - 1 | q - 1$, and so from part (a) $x^{q'-1} - 1 | x^{q-1} - 1$, so we get the divisibility we needed. Since the elements of the field $\mathbb{F}_{q'}$ are precisely the roots of the polynomial $x^{q'} - x$, and since this polynomial divides $x^q - x$, they are roots of $x^q - x$ too. Therefore, they are elements of the field \mathbb{F}_q . So $\mathbb{F}_{q'}$ is a subfield of \mathbb{F}_q .

(d) By considering degrees over \mathbb{F}_p , show that the subfields $\mathbb{F}_{q'}$ from part (c) are the only subfields of \mathbb{F}_q .

Solution: Remember that $[\mathbb{F}_q; \mathbb{F}_p] = n$, and $[\mathbb{F}_{q'}; \mathbb{F}_p] = m$. So if we have that $\mathbb{F}_{q'}$ is a subfield of \mathbb{F}_q , then we have the tower of field extensions:

$$\mathbb{F}_p \subset \mathbb{F}_{q'} \subset \mathbb{F}_q$$

By the “degrees of field extensions multiply in towers” theorem, we get that n (the degree of the top over the bottom) has to be a multiple of m (the degree of the middle over the bottom). So the only possible finite fields that are subfields of \mathbb{F}_q are the ones that we found in part (c).