MATH 100C SPRING 2016 MIDTERM SAMPLE SOLUTIONS

Instructions: There are 45 points total. Justify all of your answers, and show your work. You may use the result of one part of a problem in the proof of a later part, even if you do not complete the proof of the earlier part. You may quote basic theorems proved in the textbook or in class, unless the point of the problem is to reproduce the proof of such a theorem, or the problem tells you not to. Do not quote the results of homework exercises without reproving them. You have one hour and fifty minutes.

1 (10 pts).

(a) (5 pts). Prove Kronecker's theorem, which states that if K is a field and $f(x) \in K[x]$, then there is a field extension $K \subseteq F$ such that $f(u) = 0$ for some $u \in F$.

(b) (5 pts). Prove that if $f(x) \in K[x]$, then there exists a splitting field F for $f(x)$ over K.

(Both parts (a) and (b) are theorems proved in class and in the book; I want you to reprove them here).

Solution.

(a). The problem should have stated that $f(x)$ nonconstant of course, since a constant polynomial can't have a root in any field. So assume that $f(x) \in K[x]$ is nonconstant. Then there is some irreducible (so also nonconstant) polynomial $g(x)$ such that $f(x) = g(x)h(x)$ in $K[x]$. Now let $F = K[x]/\langle g(x)\rangle$. Since $g(x)$ is irreducible, the ideal $\langle g(x)\rangle$ of $K[x]$ is maximal as $K[x]$ is a PID. Thus F is a field. Also, we can identify K with the subfield $\{a + \langle g(x)\rangle | a \in K\}$ of F and thus we have a field extension $K \subseteq F$. Now we claim that $u = x + \langle g(x)\rangle \in F$ is a root of $g(x)$. Writing $g(x) = a_0 + a_1x + \cdots + a_nx^n$, this follows from

Date: May 2, 2016.

the calculation

$$\begin{aligned} a_0 + a_1 u + \cdots + a_n u^n &= (a_0 + \langle g \rangle) + (a_1 + \langle g \rangle)(x + \langle g \rangle) + \cdots + (a_n + \langle g \rangle)(x + \langle g \rangle)^n \\ &= a_0 + a_1 x + \cdots + a_n x^n + \langle g \rangle \\ &= g + \langle g \rangle \\ &= 0 + \langle g \rangle. \end{aligned}$$

Thus $u \in F$ is a root of $g(x)$, and hence also a root of $f(x)$ since $f(u) = g(u)h(u) = 0h(u) = 0$.

(b). If f is constant, then it has no roots so taking $F = K$ satisfies the definition of splitting field. Now we prove the result by induction on $\deg f$, where the base case is the trivial one just proved where $\deg f = 0$. Assuming now that $\deg f > 0$, by Kronecker's theorem, there is a field extension $K \subseteq L$ such that $f(x)$ has a root $r_1 \in L$. Then the subfield $K(r_1)$ of L obviously also has the root r_1 of f, so shrinking L if necessary we may assume that $L = K(r_1)$.

Then in $L[x]$, by the factor theorem we get $f(x) = (x - r_1)h(x)$ for some $h(x) \in L[x]$. Since $\deg h = \deg f - 1$, by the induction hypothesis there is a splitting field F for $h(x)$ over L. We claim that F is then a splitting field for $f(x)$ over K. First, since $h(x)$ splits over F, say $h(x) = a(x - r_2) \dots (x - r_n)$ with $r_2, \dots, r_n \in F$, we have $f(x) = a(x - r_1)(x - r_2) \dots (x - r_n)$ in $F[x]$ with $r_1, \dots, r_n \in F$. So $f(x)$ splits over F. Also, since F is the splitting field for $h(x)$ over L, we have $F = L(r_2, \dots r_n)$. Since $L = K(r_1)$, we have $F = K(r_1)(r_2, \dots, r_n) = K(r_1, \dots, r_n)$. Thus F is a splitting field for $f(x)$ over K.

2 (10 pts). Recall the theorem that a real number u is constructible if and only if there is a sequence of real numbers $u_1, \dots, u_n$, such that $u \in \mathbb{Q}(u_1, \dots, u_n)$, where $u_1^2 \in \mathbb{Q}$ and $u_i^2 \in \mathbb{Q}(u_1, \dots, u_{i-1})$ for all $2 \leq i \leq n$.

(a) (4 pts). Prove using the theorem above that if u is a constructible number, then $[\mathbb{Q}(u) : \mathbb{Q}]$ is a power of 2. (This is a result proved in class and in the book; I want you to reprove it here.)

(b) (3 pts). Prove that an angle θ is a constructible angle if and only if the angle 2θ is constructible. (Hint: $\cos(2\theta) = 2\cos^2\theta - 1$.)

(c) (3 pts). Suppose that u is a real number which is a root of the polynomial $x^4 - 4x^2 + 2$. Is u constructible? Why or why not?

Solution. (a). Let $i \geq 2$. Since $u_i^2 \in \mathbb{Q}(u_1, \ldots, u_{i-1})$, setting $a = u_i^2$, we have that u_i is a root of the polynomial $x^2 - a \in \mathbb{Q}(u_1, \ldots, u_{i-1})[x]$. Thus u_i is algebraic over $\mathbb{Q}(u_1, \ldots, u_{i-1})$ and has minimal polynomial over $\mathbb{Q}(u_1, \ldots, u_{i-1})$ of degree at most 2. Then the degree $[\mathbb{Q}(u_1, \ldots, u_{i-1})(u_i) : \mathbb{Q}(u_1, \ldots, u_{i-1})] \leq 2$ since the degree of this field extension is the same as the degree of the minimal polynomial of u_i over $\mathbb{Q}(u_1, \ldots, u_{i-1})$. Similarly, $[\mathbb{Q}(u_1) : \mathbb{Q}] \leq 2$. Now since if $K \subseteq E \subseteq F$ we have $[F : E][E : K] = [F : K]$, by induction a similar formula holds for a longer chain of field extensions. Since $\mathbb{Q} \subseteq \mathbb{Q}(u_1) \subseteq \mathbb{Q}(u_1, u_2) \subseteq \cdots \subseteq \mathbb{Q}(u_1, \ldots, u_n)$, we get

$$[\mathbb{Q}(u_1, \ldots, u_n) : \mathbb{Q}] = [\mathbb{Q}(u_1) : \mathbb{Q}][\mathbb{Q}(u_1, u_2) : \mathbb{Q}(u_1)] \ldots [\mathbb{Q}(u_1, \ldots, u_n) : \mathbb{Q}(u_1, \ldots, u_{n-1})].$$

Since this is a product of numbers which are 1 or 2, we have $[\mathbb{Q}(u_1, \ldots, u_n) : \mathbb{Q}]$ is a power of 2. Now since $u \in \mathbb{Q}(u_1, \ldots, u_n)$, we have $\mathbb{Q} \subseteq \mathbb{Q}(u) \subseteq \mathbb{Q}(u_1, \ldots, u_n)$. Then by the same formula as above $[\mathbb{Q}(u) : \mathbb{Q}]$ is a divisor of $[\mathbb{Q}(u_1, \ldots, u_n) : \mathbb{Q}]$. Since any divisor of a power of 2 is a power of 2, $[\mathbb{Q}(u) : \mathbb{Q}]$ is a power of 2.

(b). We showed in class that an angle θ is constructible if and only if the number $\cos\theta$ is a constructible number.

If $\cos\theta$ is constructible, then so is $\cos(2\theta) = 2\cos^2\theta - 1$ since the set of constructible numbers is a field. If $\cos(2\theta)$ is constructible, then we have $\cos\theta = \sqrt{\frac{\cos(2\theta)+1}{2}}$. Since the set of constructible numbers is a field and we also proved it is closed under taking square roots (this is also an immediate consequence of the theorem stated at the beginning of the problem), we see that $\cos\theta$ is also constructible.

(c). In this case, because of the special form of the polynomial, we may set $z = x^2$ and then $f = z^2 - 4z + 2$ is quadratic in z. By the quadratic formula, we get the roots of this polynomial are $z = 2 \pm \sqrt{2}$. Thus $x = \pm\sqrt{2 \pm \sqrt{2}}$, and so we have found the four roots of $f(x)$ in $\mathbb{C}$ explicity (and we see that all four roots are real). Again since the set of constructible real numbers is a field containing the rational numbers and closed under taking square roots, we see that all of the numbers $\pm\sqrt{2 \pm \sqrt{2}}$ are constructible.

(It is tempting to argue as follows: the polynomial $f(x) = x^4 - 4x^2 + 2$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion applied to the prime 2. Thus if u is a root of $f(x)$ then $\text{minpoly}_{\mathbb{Q}}(u) = f(x)$ and so $[\mathbb{Q}(u) : \mathbb{Q}] = 4$, which is a power of 2. However, we only proved that constructible numbers have degree over $\mathbb{Q}$ which is a power of 2, not the converse, so knowing that u has degree 4 over $\mathbb{Q}$ does not immediately imply that u is constructible.)

3 (5 pts). Let $K \subseteq E \subseteq F$ where K, E, and F are fields. Suppose that $K \subseteq E$ is an algebraic field extension. Show that if $u \in F$ is transcendental over K, then u is also transcendental over E.

Solution. Suppose that u is algebraic over E. Then $[E(u) : E]$ is finite, equal to the degree of the minimal polynomial of u over E. Since finite extensions are algebraic, $E \subseteq E(u)$ is an algebraic extension. Now by a theorem we proved, since $K \subseteq E$ and $E \subseteq E(u)$ are algebraic extensions, the extension $K \subseteq E(u)$ is also algebraic. By definition, this means that the element $u \in E(u)$ must be algebraic over K. This contradicts the hypothesis that u is transcendental over K.

This in fact u cannot be algebraic over E, so it must be transcendental over E as required.

4 (10 pts). Let $\zeta = e^{2\pi i/6}$ be a primitive sixth root of unity. Explicitly,

$$\zeta = \cos(\pi/3) + i\sin(\pi/3) = 1/2 + (\sqrt{3}/2)i.$$

(a) (5 pts). Show that $\mathbb{Q}(\zeta)$ is the splitting field of $f(x) = x^6 - 1$ over $\mathbb{Q}$. Prove that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$.

(b) (5 pts). Let $g(x) = x^6 - 2$. Find the splitting field F of $g(x)$ over $\mathbb{Q}$, and prove that $[F : \mathbb{Q}] = 12$.

Solution. (a) We have seen in class that over $\mathbb{C}$ the polynomial $x^6 - 1$ factors as

$$x^6 - 1 = (x - 1)(x - \zeta)\dots(x - \zeta^5).$$

(This is because the numbers $1, \zeta, \dots, \zeta^5$ are distinct and are all roots of $x^6 - 1$). Thus constructing the splitting field F of $f(x)$ inside of $\mathbb{C}$, we have $F = \mathbb{Q}(1, \zeta, \dots, \zeta^5)$. But obviously $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(1, \zeta, \dots, \zeta^5)$. The reverse inclusion $\mathbb{Q}(1, \zeta, \dots, \zeta^5) \subseteq \mathbb{Q}(\zeta)$ holds since the field $\mathbb{Q}(\zeta)$ contains ζ so must contain all powers of ζ since it is a field; but $\mathbb{Q}(1, \zeta, \dots, \zeta^5)$ is the

smallest field containing $\mathbb{Q}$ and $1, \zeta, \ldots, \zeta^5$. Thus $F = \mathbb{Q}(\zeta)$. Now since $\zeta = 1/2 + (\sqrt{3}/2)i$, we can also see that $F = \mathbb{Q}(\sqrt{3}i)$. This is a similar argument as above: clearly $\mathbb{Q}(\sqrt{3}i)$ contains the number $(1 + \sqrt{3}i)/2$, so $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\sqrt{3}i)$. Conversely $Q(\zeta)$ contains $\sqrt{3}i$ so that $\mathbb{Q}(\sqrt{3}i) \subseteq \mathbb{Q}(\zeta)$.

Now $u = \sqrt{3}i$ is a root of $x^2+3 \in \mathbb{Q}[x]$. Since $\sqrt{3}i$ is not even real, it cannot have degree 1 over $\mathbb{Q}$. Thus it has degree 2 over $\mathbb{Q}$ and $[F : \mathbb{Q}] = [\mathbb{Q}(u) : \mathbb{Q}] = 2$ (and $x^2+3 = \text{minpoly}_{\mathbb{Q}}(u)$.)

(With more work, one can also do this by showing directly that ζ satisfies a polynomial of degree 2 over $\mathbb{Q}$. To find it, one may recall that roots of polynomials with real coefficients occur in conjugate pairs. Thus any polynomial with $\mathbb{Q}$-coefficients that has ζ as a root will also have $\overline{\zeta}$ as a root. Thus since we know we are looking for a polynomial of degree 2, it must be

$$(x - \zeta)(x - \overline{\zeta}) = x^2 - (\zeta + \overline{\zeta})x + \zeta\overline{\zeta} = x^2 - (2 \operatorname{Re} \zeta)x + |\zeta|^2 = x^2 - x + 1.$$

The same calculation shows that ζ is indeed a root of this polynomial, so it must be the minimal polynomial of ζ over $\mathbb{Q}$.)

(b) We have seen in class that over $\mathbb{C}$ the polynomial $x^6 - 2$ factors as

$$x^6 - 2 = (x - \sqrt[6]{2})(x - \sqrt[6]{2}\zeta) \ldots (x - \sqrt[6]{2}\zeta^5)$$

where $\sqrt[6]{2}$ is the positive real sixth root of 2.

Then the splitting field of $x^6 - 2$ over $\mathbb{Q}$ can be constructed inside $\mathbb{C}$ as

$$F = \mathbb{Q}(\sqrt[6]{2}, \sqrt[6]{2}\zeta, \ldots, \sqrt[6]{2}\zeta^5).$$

Note that this field contains ζ also (as the ratio $\sqrt[6]{2}\zeta(\sqrt[6]{2})^{-1}$) and so $\mathbb{Q}(\zeta, \sqrt[6]{2}) \subseteq F$. On the other hand, the field $\mathbb{Q}(\zeta, \sqrt[6]{2})$ will contain $\sqrt[6]{2}\zeta^i$ for all i and so we get $F = \mathbb{Q}(\zeta, \sqrt[6]{2})$.

Now since $\sqrt[6]{2}$ satisfies $x^6 - 2$, and $x^6 - 2$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion applied at the prime 2, we see that $x^6 - 2 = \text{minpoly}_{\mathbb{Q}}(\sqrt[6]{2})$. Thus $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$. Since we already know that ζ satisfies a polynomial of degree 2 over $\mathbb{Q}$, its minimal polynomial over $\mathbb{Q}(\sqrt[6]{2})$ will be of degree 1 or 2, and the degree 1 case occurs if and only if $\zeta \in \mathbb{Q}(\sqrt[6]{2})$. But ζ is not a real number and so cannot be contained in $\mathbb{Q}(\sqrt[6]{2})$ which consists of real numbers. Thus ζ has degree 2 over $\mathbb{Q}(\sqrt[6]{2})$ and hence $[F : \mathbb{Q}(\sqrt[6]{2})] = 2$. Then

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 12.$$

5 (10 pts). Consider the field $\mathbb{Z}_3$ of integers mod 3.

(a) (3 pts). Let $I_3(n)$ be the number of irreducible polynomials of degree n over $\mathbb{Z}_3$. Calculate $I_3(1), I_3(2)$, and $I_3(4)$.

(b) (3 pts). Let $\mathbb{Z}_3 \subseteq L$ where L is a field with $|L| = 3^4 = 81$. How many $u \in L$ are there such that $\mathbb{Z}_3(u) = L$?

(c) (4 pts). Let F be the splitting field of $x^4 + 2$ over $\mathbb{Z}_3$. Find $[F : \mathbb{Z}_3]$.

Solution.

(a). Note that the problem should have defined $I_3(n)$ as the number of *monic* irreducible polynomials of degree n over $\mathbb{Z}_3$.

There are clearly 3 monic irreducible polynomials of degree 1: $x, x+1, x+2$. Since $x^9 - x$ is the product of all monic irreducible polynomials of degree 1 or 2 over $\mathbb{Z}_3$, we have $x^9 - x = (x)(x+1)(x+2)h(x)$ where $h(x)$ has degree 6 and is the product of all monic irreducible polynomials of degree 2. Thus there must be 3 monic irreducible polynomials of degree 2. Similarly, $x^{81} - x$ is the product of all monic irreducible polynomials of degree $1, 2$, or 4, so $x^{81} - x = (x^9 - x)j(x)$ where $j(x)$ has degree 72 and is the product of all irreducible monic polynomials of degree 4. So there are 18 such monic degree 4 irreducibles.

Alternatively, one may use the formula for $I_3(n)$ that comes from the mobius inversion formula. It shows that

$$I_3(1) = \sum_{d|1} \mu(1/d)3^d = \mu(1)3 = 3,$$

$$I_3(2) = (1/2)\sum_{d|2} \mu(2/d)3^d = (1/2)(\mu(2)3 + \mu(1)9) = (1/2)(-3+9) = 3,$$

$$I_3(4) = (1/4)\sum_{d|4} \mu(4/d)3^d = (1/4)(\mu(4)3 + \mu(2)9 + \mu(1)81) = (1/4)(0-9+81) = 18.$$

(b). By the theorem on subfields of finite fields, since $|L| = 3^4$, it has precisely one subfield with 3^d elements, for each d dividing 4. Thus its subfields are $\mathbb{Z}_3$, L, and a subfield E with $|E| = 9$. Now for $u \in L$, clearly $\mathbb{Z}_3(u) = L$ if and only if u is not contained in a proper subfield of L. Since $\mathbb{Z}_3 \subseteq E \subseteq L$ and these are all of the subfields of L, then $\mathbb{Z}_3(u) = L$ if and only if $u \notin E$. So there are $81 - 9 = 72$ elements $u \in L$ such that $\mathbb{Z}_3(u) = L$.

Alternatively, one may notice that $\mathbb{Z}_3(u) = L$ if and only if the minimal polyomial of u over $\mathbb{Z}_3$ has degree 4. Since $|L| = 3^4$, every element of L is a root of $x^{81} - x$ and hence

every $u \in L$ has a minimal polynomial which divides $x^{81} - x$. Thus $u \in L$ has a minimal polynomial which is of degree 1, 2, or 4, and the number of u such that $u \in L$ has a minimal polynomial of degree 4 is the same as the total number of roots of all of the irreducible polynomials of degree 4. As calculated above, there are 18 irreducible polynomials of degree 4, and each has 4 roots, for a total of 72 such elements u.

(c) (This was a homework problem).

Since x^4+2 has 1 and 2 as roots over $\mathbb{Z}_3$, we have $x^4+2 = (x+1)(x+2)h(x) = (x^2+2)h(x)$ for some $h(x) \in \mathbb{Z}_3[x]$ by the factor theorem. Polynomial long division (or just guess and check) gives $h(x) = x^2 + 1$. Then the splitting field of $x^4 + 2$ over $\mathbb{Z}_3$ is the same as the splitting field of $h(x)$ over $\mathbb{Z}_3$, since $1, 2 \in \mathbb{Z}_3$ already. Now $h(x)$ has degree 2 and is easily seen to have no roots in $\mathbb{Z}_3$. Thus it must be irreducible over $\mathbb{Z}_3$. If F is the splitting field of $h(x)$ over $\mathbb{Z}_3$, and $u \in F$ is a root of $h(x)$, then in the ring $\mathbb{Z}_3(u)[x]$ we have $h(x) = (x-u)j(x)$ and since $j(x)$ is linear $h(x)$ already splits over $\mathbb{Z}_3(u)$. So $F = \mathbb{Z}_3(u)$ and hence since u has degree 2 over $\mathbb{Z}_3$, we have $[F : \mathbb{Z}_3] = [\mathbb{Z}_3(u) : \mathbb{Z}_3] = 2$.