Math 581 Problem Set 6 Solutions

1. Let $F \subseteq K$ be a finite field extension. Prove that if $[K : F] = 1$, then $K = F$.

Proof: Let $v \in K$ be a basis of K over F. Let c be any element of K. There exists $\alpha_c \in F$ so that $c = \alpha_c v$. In particular, $1 = \alpha_1 v$ for some $\alpha_1 \in F$. However, F being a field implies $v = \alpha^{-1} \in F$. This then shows that $c \in F$ for any $c \in K$ since it is the product of two things in F. Thus, $K = F$. $\blacksquare$

2. Recall we showed that an angle θ is constructible if and only if $\cos\theta$ and $\sin\theta$ are both constructible.
(a) Show that if angles θ_1 and θ_2 are constructible, then so are angles $\theta_1+\theta_2$ and $\theta_1 - \theta_2$.

Proof: The fact that θ_1 and θ_2 are constructible means that $\cos\theta_i$ and $\sin\theta_i$ are both constructible for $i = 1, 2$. We know that the set of constructible numbers forms a field, so we can add and multiple the values to get constructible numbers. The fact that $\theta_1 + \theta_2$ and $\theta_1 - \theta_2$ are constructible then follows from the trig identities:

$$\begin{aligned} \sin(\theta_1 \pm \theta_2) &= \sin\theta_1 \cos\theta_2 \pm \cos\theta_1 \sin\theta_2 \\ \cos(\theta_1 \pm \theta_2) &= \cos\theta_1 \cos\theta_1 \mp \sin\theta_1 \sin\theta_2 \end{aligned}$$

since everything on the right is now constructible. $\blacksquare$

(b) Prove that if the regular mn-gon is constructible, i.e., one can construct an angle of $\frac{2\pi}{mn}$, then the regular m- and n-gons are constructible as well.

Proof: The point to observe here is that $\frac{2\pi}{m} = \frac{2\pi}{mn} + \cdots + \frac{2\pi}{mn}$ where there are n-copies of $\frac{2\pi}{mn}$ in the sum. Now use induction and part (a) to conclude that $\frac{2\pi}{m}$ is constructible. Similarly for $\frac{2\pi}{n}$. $\blacksquare$

(c) Prove that if $\gcd(m, n) = 1$ and the regular m- and n-gons are both constructible, then the regular mn-gon is constructible.

Proof: The fact that $\gcd(m, n) = 1$ implies that there exists $a, b \in \mathbb{Z}$ so that $am+bn=1$. Now we have

$$\begin{aligned}\frac{2\pi}{mn} &= 1\cdot\left(\frac{2\pi}{mn}\right)\\ &= (am+bn)\cdot\left(\frac{2\pi}{mn}\right)\\ &= a\left(\frac{2\pi}{n}\right)+b\left(\frac{2\pi}{m}\right).\end{aligned}$$

Now apply induction and part (a) to conclude that $\frac{2\pi}{mn}$ is constructible. ■

(d) Show it is possible to trisect the angle $\frac{2\pi}{5}$ and construct a regular 15-gon.

Proof: Observe that the 3-gon is constructible because $\frac{2\pi}{3}$ is constructible since $\cos\frac{2\pi}{3}=-\frac{1}{2}$ and $\sin\frac{2\pi}{3}=\frac{\sqrt{3}}{2}$. We know the constructible numbers form a field and that we can take square roots of constructible numbers to get another constructible number, so it is clear these are both constructible. If we can show that $\frac{2\pi}{5}$ is constructible, we will have that a 15-gon is constructible by part (c). Observe that $\cos\frac{2\pi}{5}=\frac{1}{4}(-1+\sqrt{5})$ and $\sin\frac{2\pi}{5}=\frac{1}{2}\sqrt{\frac{1}{2}(5+\sqrt{5})}$. These are both formed by taking square roots and field operations from constructible numbers, so are constructible. ■

3. Recall deMoivre's theorem from section 2.3: For any integer n one has $(\cos\theta+i\sin\theta)^n=\cos n\theta+i\sin n\theta$.
(a) Use deMoivre's theorem to find a formula for $\sin 7\theta$ that does not contain any $\cos\theta$'s.

First observe that the imaginary part of deMoivre's formula gives

$$\sin 7\theta = -\sin^7\theta+21\cos^2\theta\sin^5\theta-35\cos^4\theta\sin^3\theta+7\cos^6\theta\sin\theta.$$

Using that $\cos^2\theta=1-\sin^2\theta$ we obtain

$$\sin 7\theta=-64\sin^7\theta+112\sin^5\theta-56\sin^3\theta+7\sin\theta.$$

(b) Plug in $\theta=\frac{2\pi}{7}$ to find a polynomial in $\mathbb{Z}[x]$ that has $\sin\left(\frac{2\pi}{7}\right)$ as a root.

Plugging in $\theta=\frac{2\pi}{7}$ we obtain that $\sin\left(\frac{2\pi}{7}\right)$ is a root of the polynomial

$$f(x)=64x^7-112x^5+56x^3-7x.$$

Thus, $\sin\left(\frac{2\pi}{7}\right)$ is a root of the polynomial

$$g(x) = 64x^6 - 112x^4 + 56x^2 - 7.$$

(c) Prove that the polynomial you found in part (b) is irreducible in $\mathbb{Z}[x]$.

Proof: We see that $g(x)$ is irreducible by using Eisenstein with $p = 7$. ■

(d) Prove that the regular heptagon (7-gon) is not constructible.

Proof: Using part (c) we see that $\left[\mathbb{Q}\left[\sin\left(\frac{2\pi}{7}\right)\right] : \mathbb{Q}\right] = 6$. Since this is not a power of 2, it must be that $\sin\left(\frac{2\pi}{7}\right)$ is not constructible. Hence, we cannot construct a regular 7-gon. ■

4. (a) Show that $x^4 + x + \overline{1}$ is irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$.

Proof: Note that this has no roots in $\mathbb{Z}/2\mathbb{Z}$ as observed by plugging in $\overline{0}$ and $\overline{1}$. To show it is irreducible we need to use the method of undetermined coefficients to show it does not factor into quadratics. Since the only possibilities for coefficients are $\overline{0}$ and $\overline{1}$ we immediately see the quadratics must be of the form

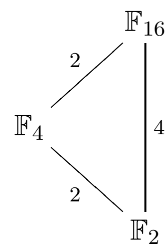
$$x^4 + x + \overline{1} = (x^2 + ax + \overline{1})(x^2 + bx + \overline{1}).$$

This gives that $b + c = \overline{0}$ for the coefficient of x^3 and $b + c = \overline{1}$ for the coefficient of x, a contradiction. Thus $x^4 + x + 1$ is irreducible. ■

(b) Use part (a) to construct a finite field $\mathbb{F}_{2^4}$ of order 16.

Recall $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Note that since $x^4+x+\overline{1}$ is irreducible, $\mathbb{F}_2[x]/\langle x^4+x+1\rangle$ is a field. It has a basis of $\{1, \overline{x}, \overline{x}^2, \overline{x}^3\}$. Thus, elements in this field are of the form $a_0 + a_1\overline{x} + a_2\overline{x}^2 + a_3\overline{x}^3$ with $a_i \in \mathbb{F}_2$. Hence, there are 2^4 elements in this field.

(c) Draw a diagram that shows all the subfields of $\mathbb{F}_{2^4}$.



5. Let F be a field of characteristic p.
(a) Prove that for every positive integer n, one has

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

for all $a, b \in F$. (Hint: use induction on n.)

Proof: The case of $n = 1$ has been proven in previous homework sets for $\mathbb{Z}/p\mathbb{Z}$ by observing all the middle binomial coefficients are divisible by p. The same argument gives the result for $n = 1$ in this case. Now assume that for some $k \in \mathbb{N}$ we have

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

for all $a, b \in F$. Raising both sides to the p we have

$$\begin{aligned} (a+b)^{p^{k+1}} &= (a^{p^k} + b^{p^k})^p \\ &= a^{p^{k+1}} + b^{p^{k+1}} \end{aligned}$$

where the last equality follows from the $n = 1$ case. Thus, we have the result for all n by induction. ■

(b) Now assume that in addition F is finite. Prove that the map $\phi : F \to F$ given by $\phi(a) = a^p$ is an isomorphism. Use this to conclude that every element of F has a p^{th} root in F.

Proof: First we prove that ϕ is a homomorphism. Let $a, b \in F$. Then we have $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$ where we have used that elements commute since this is a field. Now, $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$ by part (a). It is also clear that $\phi(1_F) = 1_F$. Thus, ϕ is a homomorphism.

The fact that ϕ is injective is easy to show. Suppose $\phi(a) = 0_F$. Then $a^p = 0_F$ which implies $a = 0_F$ since F is necessarily an integral domain. Thus $\ker\phi = \langle 0_F \rangle$ and so ϕ is injective. Now we use that F is a finite set and Homework set 1 problem 2 to conclude ϕ is also surjective.
Let $a \in F$. Then there exists a $b \in F$ so that $\phi(b) = a$ since ϕ is surjective, i.e., $b^p = a$. Thus every element in F is a p^{th} root. Note that by looking at ϕ composed with itself m times for any $m \in \mathbb{N}$ we get every element is a p^m power. $\blacksquare$

(c) Let K be a finite field of characteristic p with $F \subset K$ and m a positive integer. Set $L = \{a \in K : a^{p^m} \in F\}$. Prove that L is a subfield of K that contains F.

Proof: There are two things to prove here, that L contains F and that L is a subfield of K. It is clear that $F \subseteq L$ as any element that is in F satisfies that its p^m power is still in F as F is closed under multiplication. To see L is a subfield we need to show it is closed under addition, multiplication, and inversion. Let $a, b \in L$. From part (a) we have that $(a+b)^{p^m} = a^{p^m} + b^{p^m}$. Since $a, b \in L$, we have that a^{p^m} and b^{p^m} are both in F, hence there sum is as well. Thus $(a+b)^{p^m} \in F$ and hence $a + b \in L$. To see multiplication, $(ab)^{p^m} = a^{p^m} b^{p^m} \in F$ and so $ab \in L$. Let $a \in L$, i.e., $a^{p^m} \in F$. Since $L \subseteq K$ we know that there exists $b \in K$ such that $ab = 1$. Using that $a^{p^m} b^{p^m} = (ab)^{p^m} = 1$ we see that b^{p^m} is necessarily the inverse of a^{p^m} in F since F is a field, $a^{p^m} \in F$ and inverses are unique. Thus, $b^{p^m} \in F$ and thus $b \in L$. Thus, L is a subfield of K. $\blacksquare$

(d) Prove $L = F$. (Hint: Think vector spaces. If $\{v_1, \ldots, v_n\}$ is a basis of L over F, use parts (a) and (b) to prove that $\{v_1^{p^m}, \ldots, v_n^{p^m}\}$ is linearly independent over F, which implies $n = 1$.)

Proof: Let $\{v_1, \ldots, v_n\}$ be a basis of L over F. Suppose that $\{v_1^{p^m}, \ldots, v_n^{p^m}\}$ is linearly dependent, i.e., there exists $a_1, \ldots, a_n$ in F not all zero so that

$$a_1 v_1^{p^m} + \cdots + a_n v_n^{p^m} = 0.$$

Part (b) gives that for each $a_i \in F$ there exists an $\alpha_i \in F$ so that $a = \alpha_i^{p^m}$. Thus, we have

$$\alpha_1^{p^m} v_1^{p^m} + \cdots + \alpha_n^{p^m} v_n^{p^m} = 0.$$

Now we apply part (a) to conclude that

$$\begin{aligned} 0 &= \alpha_1^{p^m} v_1^{p^m} + \cdots + \alpha_n^{p^m} v_n^{p^m} \\ &= (\alpha_1 v_1 + \cdots + \alpha_n v_n)^{p^m}. \end{aligned}$$

Since L is a field, we have that this implies

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0.$$

But this contradicts the fact that $\{v_1, \ldots, v_n\}$ is a linearly independent set. Thus it must be that $\{v_1^{p^m}, \ldots, v_n^{p^m}\}$ is a linearly independent set as well. However, we know that $v_i^{p^m} \in F$ for $1 \leq i \leq n$ by the definition of L. Thus, it must be that $n = 1$ and $L = F$. $\blacksquare$

6. Write a critique of the "proof" given in the following article. Please use only material the author provides in the article to critique the proof.

http://www.washingtonpost.com/wp-dyn/content/blog/2006/02/15/BL2006021501989.html