Math 114 Homework 3 Michael Knopf
(due Thursday, 19 February)

1. Prove that if F is a field, K is an algebraic closure of F, and E is an algebraic extension of F, then there is an injective homomorphism $E \hookrightarrow K$ which fixes F. Give an example (with proof) to illustrate that there may be more than one such homomorphism.

Proof. For algebraic extensions E/F and K/F, define an *embedding* of F into K to be any homomorphism $\varphi : E \to K$ such that $\varphi \restriction_F = id$. Note that an embedding must be injective, since it restricts to the identity on F so it cannot be the zero map.

Let $\mathcal{S} = \{(H, \varphi) : F \subseteq H \subseteq E, \varphi : H \to K \text{ is an embedding}\}$. Define an order relation on $\mathcal{S}$ by $(H, \varphi) \preceq (H', \varphi')$ if $H \subseteq H'$ and $\varphi' \restriction_H = \varphi$. Now, let $(H_i, \varphi_i)_{i\in I}$ be a chain in $\mathcal{S}$. Now, consider the pair $\left(\bigcup_{i\in I} H_i, \bigcup_{i\in I} \varphi_i\right) \in \mathcal{S}$ (a function is a relation, so here we are taking the union of functions to be their union as relations).

Since, for any x in the domain of both φ_i and φ_j for some $i, j \in I$, we have $\varphi_i(x) = \varphi_j(x)$ (since one of these maps restricts to the other), $\bigcup_{i\in I} \varphi_i$ is a well-defined function from $\bigcup_{i\in I} H_i$ to K. Also, this function is a homomorphism, since for any $x, y \in \bigcup_{i\in I} H_i$ there is some H_i such that $x, y \in H_i$. Thus, the images of $x+y$ and xy under $\bigcup_{i\in I} \varphi_i$ are their images under φ_i, which is a homomorphism. Clearly, $\bigcup_{i\in I} \varphi_i$ is injective, since it still restricts to the identity on F. So $\bigcup_{i\in I} \varphi_i$ is an embedding of F into K. Also, $H_i \subseteq \bigcup_{i\in I} H_i$ for all $i \in I$. Thus $(\bigcup_{i\in I} H_i, \bigcup_{i\in I} \varphi_i)$ is an upper bound for $\mathcal{S}$. So, by Zorn's Lemma, $\mathcal{S}$ contains some maximal element (H, φ).

Now, suppose that $H \neq E$. Then there exists some $\alpha \in E \setminus H$. Since E is algebraic over F, α is algebraic over F, thus also over H. So let $m_\alpha(x)$ be its minimal polynomial over H. Since φ is a homomorphism on H, it extends to a homomorphism $\widetilde{\varphi} : H[x] \to K[x]$ defined by $\widetilde{\varphi}(a_k x^k + \cdots a_1 x + a_0) = \varphi(a_k)x^k + \cdots \varphi(a_1)x + \varphi(a_0)$. Since K is an algebraic closure of F, it must contain some element β which is a root of $\widetilde{\varphi}(m_\alpha(x))$.

Now, letting n be the degree of α over H, we know that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a basis for $H(\alpha)$ over H. So for every $\gamma \in H[x]$, there is a unique polynomial $p(x) \in H[x]$ of degree less than n such that $\gamma = p(\alpha)$. So we may uniquely identify elements of $H[x]$ with these corresponding polynomials, evaluated at α.

Thus, we can define a map $\psi : H(\alpha) \to K$ by $\psi(p(\alpha)) = p(\beta)$. Now, suppose $p, q \in H[x]$. Then $\psi(p(\alpha) + q(\alpha)) = \psi((p+q)(\alpha) = (p+q)(\beta) = p(\beta) + q(\beta) = \psi(p(\alpha)) + \psi(q(\alpha))$, since $(p+q)(x)$ still has degree less than n.

The only trouble arises when we try to compute $\psi((p \cdot q)(\alpha)$, since $(p \cdot q)(x)$ could have degree greater than or equal to n. However, if we just take polynomial multiplication modulo m_α in $H[x]$ and $K[x]$, then we see that the map is multiplicative as well. This is valid because $p(\alpha) = (p \bmod m_\alpha)(x)$ in both $H[x]$ and $K[x]$. Thus ψ is a homomorphism.

Clearly, ψ restricts to the identity on H because, if $\gamma \in H$, then $\gamma = p_\gamma(\alpha)$ for the constant polynomial $p_\gamma(x) = \gamma$. So $\psi(\gamma) = \psi(p_\gamma(\alpha)) = p_\gamma(\beta) = \gamma$. Thus ψ is an embedding of $H(\alpha)$ into K. Therefore, $(H, \varphi) \prec (H(\alpha), \psi)$, contradicting the maximality of (H, φ). So $H = E$, and thus φ is an embedding, i.e. an injective homomorphism, of E into K.

To see that these embeddings are not necessarily unique, consider the chain of subfields $\mathbb{R} \subseteq \mathbb{R}(i) \subseteq \mathbb{C}$. i solves the polynomial $x^2 + 1 \in \mathbb{R}[x]$, so $\mathbb{R}(i)/R$ is an algebraic extension. One embedding of $\mathbb{R}(i)$ into $\mathbb{C}$ is the identity map. Another is given by conjugation, which we have already shown in lecture to be an automorphism of $\mathbb{C}$ that fixes $\mathbb{R}$. So clearly conjugation, when restricted to the subfield $\mathbb{R}(i)$, is still a homomorphism which fixes $\mathbb{R}$, thus an embedding of $\mathbb{R}$ into $\mathbb{C}$.

□

2. (Exercise 2 in DF §13.5.) Find all irreducible polynomials of degrees 1, 2, and 4 over $\mathbf{F}_2$, and prove that their product is $X^{16} - X$.

Proof. Obviously, any degree 1 polynomial is irreducible, and x and $x+1$ are the only degree 1 polynomials over $\mathbb{F}_2$. Now, suppose $p(x) = a_n x^n + \cdots a_1 x + a_0$ is irreducible over $\mathbb{F}_2$, and has degree $n > 1$. Since its degree is n, we must have $a_n = 1$.

If $p(x)$ has a root, then it has a linear factor. So $a_0 = 1$, else 0 is a root. Also, we must have $a_{n-1} + \cdots + a_1 = 1$, or else $p(1) = 1 + a_{n-1} + \cdots + a_1 + 1 = a_{n-1} + \cdots + a_1 = 0$. If $n = 2$, this means $a_1 = 1$. So the only possibility is x^2+x+1. If $n=4$, then we need an odd number of the coefficients a_1, a_2, and a_3 to be 1. This leaves as possibilities x^4+x+1, x^4+x^2+1, x^4+x^3+1, and $x^4+x^3+x^2+x+1$.

x^4+x^2+1 can be factored as $(x^2+x+1)^2$. Since the other three degree 4 polynomials do not have roots, they do not have linear factors. So if they can be factored, then their only factors are irreducible quadratics (since if it had an factor of degree 3 then it would also have a factor of degree 1). However, the only irreducible quadratic is (x^2+x+1), and we have already shown that its square is not any of the three remaining polynomials. So these are all irreducible, thus the irreducible polynomials of degree 1, 2, or 4 over $\mathbb{F}_2$ are

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

By proposition 18 in section 14.3, the polynomial $x^{p^n}-x$ is precisely the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d, where d runs through all the divisors of n. Thus $x^{16}-x=x^{2^4}-x$ is exactly the product of these 6 irreducible polynomials.

□

Note: We will use the following facts in the next two problems:

(a) For any n in the prime subfield of a field of characteristic p, $n^p=n$.

Proof. In a field F of characteristic p, the nonzero elements of the prime subfield form a multiplicative group of order p. So $n^p=n^{p-1}n=1\cdot n=n$ for any n in the prime subfield of F. □

(b) For any $a_1,\dots,a_n$ in a field of characteristic p, $(a_1+\dots+a_n)^p=a_1^p+\dots+a_n^p$.

Proof. For $n=2$, this is Proposition 35 in D&F. Now suppose this is true for some n.
Then $(a_1+\dots+a_n+a_{n+1})^p=(a_1+\dots+a_n)^p+a_{n+1}^p=a_1^p+\dots+a_{n+1}^p$. □

(c) If $q(x)\in F[x]$, of degree k, has roots $\alpha_1,\dots,\alpha_k$ (not necessarily distinct) in a splitting field K, then the coefficient of x^{n-1} in any degree n divisor of $q(x)$ is $-(\alpha_{i_1}+\dots+\alpha_{i_n})$ for some $i_1,\dots,i_n\in\{1,\dots,k\}$.

Proof. $q(x)$ factors over K as $q(x)=(x-\alpha_1)\cdots(x-\alpha_k)$. Let $r(x)$ be any divisor of $q(x)$ over K, and let n be the degree of $r(x)$. We will now show by induction on n that the coefficient of x^{n-1} in $r(x)$ is $-(\alpha_{i_1}+\dots+\alpha_{i_n})$ for some $i_1,\dots,i_n\in\{1,\dots,p\}$.

This is vacuously true if $n=0$, since then there is no x^{n-1} term. Now assume the propoosition is true for some n. If $n=k$, then there are no degree $n+1$ divisors, so assume $n<k$. By the inductive hypothesis, all divisors of $q(x)$ of degree $n+1$ are of the form $(x^n-(\alpha_{i_1}+\dots+\alpha_{i_n})x^{n-1}+\beta_{n-2}x^{n-2}+\dots+\beta_1x+\beta_0)(x-\alpha_j)$ for some $\beta_1,\dots,\beta_{n-2}$. Expanding this polynomial gives $x^{n+1}-(\alpha_{i_1}+\dots+\alpha_{i_n}+\alpha_j)x^n+\dots-\beta_0\alpha_j$. So the coefficient of x^n is in fact of this form. □

3. (Exercise 5 in DF §13.5.) For any prime p and any nonzero $a\in\mathbf{F}_p$ prove that X^p-X+a is irreducible and separable over $\mathbf{F}_p$. (Hint for the irreducibility: One approach—prove first that if α is a root then $\alpha+1$ is also a root. Another approach—suppose it's reducible and compute derivatives.)

Proof. Let K be a splitting field for $q(x)=x^p-x+a$ over $\mathbb{F}_p$. If some $\alpha\in K$ is a root of $q(x)$, then we have

$$(\alpha+1)^p-(\alpha+1)+a=\alpha^p+1^p-\alpha-1+a=\alpha^p-\alpha+a=0$$

so $\alpha+1$ is also a root of $q(x)$. By inductive application of this fact, we see that $\alpha+k$ is a root, for any $k\in\mathbb{F}_p$.

Therefore, if $\alpha\in\mathbb{F}_p$ is a root of $q(x)$, then $\alpha+(a-\alpha)=a$ must also be a root. However, this implies that $a^p-a+a=a^p=a=0$, a contradiction. So $q(x)$ has no roots in $\mathbb{F}_p$.

Let the roots of $q(x)$ be $\alpha_1,\dots,\alpha_p\in K$. These roots must be distinct, since WLOG $\alpha_{i+1}=\alpha_i+1$, by the fact derived in the first paragraph. **So $q(x)$ is separable**. By fact (c) in the note above, any nonunit divisor of degree $n < p$ must contain a term with coefficient $-(\alpha_{i_1} + \cdots + \alpha_{i_n})$ for some $i_1, \cdots, i_n \in \{1, \cdots, p\}$. Note that

$$\begin{aligned} q\left(\frac{\alpha_{i_1} + \cdots + \alpha_{i_n}}{n}\right) &= \left(\frac{\alpha_{i_1} + \cdots + \alpha_{i_n}}{n}\right)^p - \frac{\alpha_{i_1} + \cdots + \alpha_{i_n}}{n} + a \\ &= \frac{\alpha_{i_1}^p + \cdots + \alpha_{i_n}^p}{n^p} - \frac{\alpha_{i_1} + \cdots + \alpha_{i_n}}{n} + \frac{na}{n} \\ &= \frac{(\alpha_{i_1}^p - \alpha_{i_1} + a) + \cdots + (\alpha_{i_n}^p - \alpha_{i_n} + a)}{n} = 0. \end{aligned}$$

Therefore, if this coefficient $-(\alpha_{i_1} + \cdots + \alpha_{i_n})$ is in $\mathbb{F}_p$, then $\frac{\alpha_{i_1} + \cdots + \alpha_{i_n}}{n} \in \mathbb{F}_p$ is a root of $q(x)$, which contradicts the fact that $q(x)$ has no roots in $\mathbb{F}_p$. Thus, no nonunit divisor of $q(x)$ with degree less than p can have all of its coefficients in $\mathbb{F}_p$, thus $q(x)$ **is irreducible over** $\mathbb{F}_p$.

□

4. (Exercise 7 in DF §13.5.) Suppose K is a field of characteristic $p > 0$ which is not a perfect field; that is, the Frobenius map $K \to K$ given by $\alpha \mapsto \alpha^p$ is not surjective. Prove there exist irreducible inseparable polynomials over K. Conclude that there exist inseparable finite extension of K.

Proof. Let $a \in K$ be some element which is not in the image of the Frobenius map, i.e. a is not a pth power in K. Let $q(x) = x^p - a$. Since $D_x(q(x)) = px^{p-1} = 0$, any root of $q(x)$ is also a root of $D_x(q(x))$, thus $q(x)$ **is inseparable**, since every root of has multiplicity at least 2.

Now, let H be a splitting field for $q(x)$ over K, so that there exist roots $\alpha_1, \ldots, \alpha_p \in H$ (not all unique) of $q(x)$. Note that, for all i, $\alpha_i \notin K$ or else α_i would map to a under the Frobenius map, a contradiction.

Assume that some nonunit divisor $r(x)$ of $q(x)$ has degree $n < p$. Then, by fact (c) in the note above, the coefficient of the second term in $r(x)$ is $-(\alpha_{i_1} + \cdots + \alpha_{i_n})$ for some $i_1, \ldots, i_n \in \{1, \cdots, p\}$. Note that

$$\left(\frac{\alpha_{i_1} + \cdots + \alpha_{i_n}}{n}\right)^p = \frac{\alpha_{i_1}^p + \cdots + \alpha_{i_n}^p}{n^p} = \frac{na}{n} = a,$$

Therefore, if this coefficient $-(\alpha_{i_1} + \cdots + \alpha_{i_n})$ is in K, then $\frac{\alpha_{i_1} + \cdots + \alpha_{i_n}}{n} \in K$ is a root of $q(x)$, which contradicts the fact that $q(x)$ has no roots in K. Thus, no nonunit divisor of $q(x)$ with degree less than p can have all of its coefficients in K, thus $q(x)$ **is irreducible over** K.

Since $q(x)$ is irreducible, $K/(q(x))$ is a field which contains a root of $q(x)$. However, $q(x)$ is inseparable, so $K/(q(x))$ is an inseparable, algebraic (thus finite) extension of K.

□

5. (Exercise 5 in DF §14.3.) Exhibit an explicit isomorphism between the splitting fields of $X^3 - X + 1$ and $X^3 - X - 1$ over $\mathbf{F}_3$.

Proof. We have shown in problem 3 that $x^p - x + a$ is irreducible for any $a \in \mathbb{F}_p$, and that if α is a root of this polynomial then so is $\alpha + k$ for any $k \in \mathbb{F}_p$. Thus, both of these polynomials are irreducible over $\mathbb{F}_3$, and if α is a root of one, then so are $\alpha + 1$ and $\alpha + 2$.

Let α and β be roots of $x^3 - x + 1$ and $x^3 - x - 1$, respectively. Then $\mathbb{F}_3(\alpha)$ and $\mathbb{F}_3(\beta)$ are splitting fields for these polynomials, since they each contian the three distinct roots.

Define a homomorphism $\varphi : \mathbb{F}_3(\alpha) \to \mathbb{F}_3(\beta)$ by

$$a + b\alpha + c\alpha^2 \mapsto a - b\beta + c\beta^2.$$

Then $\varphi((a + b\alpha + c\alpha^2) + (d + e\alpha + e\alpha^2) = \varphi((a + d) + (b + e)\alpha + (c + e)\alpha^2) = (a + d) - (b + e)\beta + (c + e)\beta^2 = \varphi(a + b\alpha + c\alpha^2) + \varphi(d + e\alpha + e\alpha^2)$, so the map is additive. Now check that the map is multiplicative:

$$\varphi((a + b\alpha + c\alpha^2)(d + e\alpha + f\alpha^2))$$

$$
\begin{aligned}
&= ad + bd\alpha + ae\alpha + cd\alpha^2 + be\alpha^2 + af\alpha^2 + ce\alpha^3 + bf\alpha^3 + cf\alpha^4 \\
&= ad + bd\alpha + ae\alpha + cd\alpha^2 + be\alpha^2 + af\alpha^2 + bf(\alpha - 1) + ce(\alpha - 1) + cf(\alpha - 1)\alpha \\
&= (ad - bf - ce) + (ae + bd + bf + ce - cf)\alpha + (af + be + cd + cf)\alpha^2 \\
&= (ad - bf - ce) - (ae + bd + bf + ce - cf)\beta + (af + be + cd + cf)\beta^2
\end{aligned}
$$

and

$$\varphi(a + b\alpha + c\alpha^2)\varphi(d + e\alpha + f\alpha^2)$$

$$
\begin{aligned}
&= (a - b\beta + c\beta^2)(d - e\beta + f\beta^2) \\
&= ad - bd\beta - ae\beta + cd\beta^2 + be\beta^2 + af\beta^2 - ce\beta^3 - bf\beta^3 + cf\beta^4 \\
&= ad - bd\beta - ae\beta + cd\beta^2 + be\beta^2 + af\beta^2 - ce(\beta + 1) - bf(\beta + 1) + cf(\beta + 1)\beta \\
&= ad - ae\beta + af\beta^2 - bd\beta + be\beta^2 - bf\beta - bf + cd\beta^2 - ce\beta - ce + cf\beta^2 + cf\beta \\
&= (ad - bf - ce) - (ae + bd + bf + ce - cf)\beta + (af + be + cd + cf)\beta^2
\end{aligned}
$$

so φ is a homomorphism.

If $\varphi(a + b\alpha + c\alpha^2) = a - b\beta + c\beta^2 = 0$, then $a = b = c = 0$ because $\{1, \beta, \beta^2\}$ is linearly independent over $\mathbb{F}_3$. Therefore, φ is injective. Since $\mathbb{F}_3(\alpha)$ and $\mathbb{F}_3(\beta)$ are both extensions of degree 3 over $\mathbb{F}_3$, they both have cardinality 3^3, so φ must also be surjective, thus an isomorphism.

□

6. (Exercise 11 in DF §14.3.) Prove that $X^{p^n} - X + 1$ is irreducible over $\mathbf{F}_p$ only when $n = 1$ or $n = p = 2$. (Hint: Note that if α is a root, then so is $\alpha + a$ for any $a \in \mathbf{F}_{p^n}$. Show that this implies that $\mathbf{F}_p(\alpha)$ contains $\mathbf{F}_{p^n}$ and that $[\mathbf{F}_p(\alpha) : \mathbf{F}_{p^n}] = p$.)

Proof. Let α be a root of $x^{p^n} - x + 1$, and let $a \in \mathbb{F}_{p^n}$. Then, by the identity used in the proof of the existence and uniqueness of finite fields,

$$(\alpha + a)^{p^n} - (\alpha + a) + 1 = (\alpha^{p^n} - \alpha + 1) + (a^{p^n} - a) = 0$$

so $\alpha + a$ is also a root of $x^{p^n} - x + 1$.

Now assume that $x^{p^n} - x + 1$ is irreducible over $\mathbb{F}_p$. Since $\mathbb{F}_p(\alpha)$ is an algebraic extension, it is finite. Thus it is isomorphic to $\mathbb{F}_{p^m}$ for some m, so it is a Galois extension. Therefore, by proposition 13 in section 14.2, it must contain every root of $x^{p^n} - x + 1$, because it contains one of the roots. So $\alpha + a \in \mathbb{F}_p(\alpha)$ for all $a \in \mathbb{F}_{p^n}$, so also $a = (\alpha + a) - \alpha \in \mathbb{F}(\alpha)$. Thus $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$.

Since the polynomial, which we have assumed to be irreducible over $\mathbb{F}_p$, has degree p^n, $\mathbb{F}_p(\alpha)$ is a degree p^n extension. Thus the number of elements in this field is $(p^n)^p = p^{np}$. As a vector space over $\mathbb{F}_{p^n}$, then, it must have degree p, since the number of elements in a vector space over a field with pn elements is k^{pn}, where k is the dimension of the space. Also, the degree of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is n. So

$$p^n = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_p(\alpha) : \mathbb{F}_{p^n}][\mathbb{F}_{p^n} : \mathbb{F}_p] = np.$$

This equation is satisfied only when $n = 1$ or $n = p = 2$.

□