M622 Selected solutions from homework collected Tuesday (March 7).

1. Suppose d and n are integers, α is either x or a positive integer greater than 1.

   Of course $\alpha^n - 1 = (\alpha^d - 1)\alpha^{n-d} + \alpha^{n-d} - 1$. Thus, $\alpha^d - 1|\alpha^n - 1$ if and only if $\alpha^d - 1|\alpha^{n-d} - 1$.

   Claim 1 *With d, n, α as above, $\alpha^d - 1|\alpha^n - 1$ if and only if $d|n$.*

   Proof. Fix d. If $n = 1$, it is obvious that $\alpha^d - 1|\alpha - 1$ if and only if $d = 1$, which divides $n = 1$. Assume for all integers m strictly less than n that the claim holds. But $\alpha^d - 1|\alpha^n - 1$ if and only if $\alpha^d - 1|\alpha^{n-d} - 1$ if and only if $d|n$—the first logical equivalence by the sentence before the claim, and the second from the induction hypothesis. This completes the proof.

   Application: Classification of all subfields of the field F_{p^n}:

   Let $n \in \mathbb{N}$. As we observed $F_{p^n} - \{0\}$ is cyclic. If $n \geq d$, and F_{p^d} is a subfield, then $F_{p^d} - \{0\}$ is a subgroup of $F_{p^n} - \{0\}$, which means that $p^d - 1|p^n - 1$. By the paragraph above, $d|n$. So we've put a restriction on the possible subfields of F_{p^n}. Do we know that if $d|n$, then there exist a subfield isomorphic to F_{p^d}? We do have a unique (using cyclicity) subgroup G of $F_{p^n} - \{0\}$ having $p^d - 1$ elements. Note that any element $b \in G \cup \{0\}$ is a root of $x^{p^d} - x$, and, conversely, $G \cup \{0\}$ is the complete set of roots of $x^{p^d} - x$. It is not difficult to show $G \cup \{0\}$ is closed under multiplication (G is obviously closed closed multiplication, so $G \cup \{0\}$ is closed under multiplication) and addition (use Froebenius) —it's a subfield, one having p^d elements, capping off the proofs of two exercises.

2. For that interesting problem 5. **BE SURE YOU READ THIS BEFORE CLASS tomorrow. Thanks!**

   Let S be the splitting field for $t(x) \in F[x]$, and let $b \in S$ be a root of an irreducible polynomial $m(x) \in F[x]$. Suppose the roots of $t(x)$ are $\{r_1, \ldots, r_k\}$. Let T be the splitting field of $m(x)t(x)$, a field that can be formed by extending S, and let c be a root of $m(x)$. So $c \in T$.

   As we've seen $F(b) \cong F(c)$, via an isomorphism σ that fixes F pointwise, and $F(c)$ can be extended to a splitting field S' of $t(x)$ in such a way that S and S' are isomorphic via an isomorphism that extends σ. Since all roots of $t(x)$ and $m(x)$ are contained in T, the construction can be effected in T. Indeed, $S = F(b, r_1, \ldots, r_k) = F(r_1, \ldots, r_k)$ (since $b \in S$, and$F(b_1, \ldots, r_k) = S$), and just as $S = F(c, r_1, \ldots, r_k)$, we have $S' = F(c, r_1, \ldots, r_k)$. But there is only one splitting field of $t(x)$ in T, namely $F(r_1, \ldots, r_k) = S$. That is, $S = S'$, which means that $c \in F(r_1, \ldots, r_k)$. It follows that are all roots of $m(x) \in F[x]$ are contained in S, completing the proof.

The other direction: Suppose K/F is an extension satisfying the following: $[K : F] = n \in \mathbb{N}$, and whenever $m(x) \in F[x]$ is irreducible and K contains a root b of $m(x)$, then K splits $m(x)$ (that is, all roots of $m(x)$ are contained in K. Then K is a splitting field of some polynomial $t(x) \in F[x]$:

Since $[K : F]$ is finite, it is not difficult to see that there exists a finite set $\{k_1, \ldots, k_s\} \subseteq K$ such that $K = F(k_1, \ldots, k_s)$. For $i = 1, \ldots, s$, let $m_i(x) \in F[x]$ be the minimal polynomial of k_i. Consider $t(x) = m_1(x) \ldots m_k(x)$. Since $m_i(x)$ is irreducible, and $k_i \in K$ is a root of $m_i(x)$, by hypothesis, $m_i(x)$ factors completely in K. Those K splits $t(x)$. If J is a field, $F \leq J \leq K$, and J splits $t(x)$, then contains all roots of $m_i(x)$, so J contains k_i—so J contains $\{k_1, \ldots, k_s\}$. But $K = F(k_1, \ldots, k_s) \subseteq J$; hence, $K = J$. Thus J is the splitting field of $t(x)$, completing the proof.

3. Problems involving splitting fields of various polynomials in $\mathbb{Q}[x]$, and their degree over $\mathbb{Q}$.

   (a) $a(x) = x^4 + 2$. First, let's find the roots. We solve $(Re^{i\theta})^4 = -2 = 2e^{i\pi}$ (since $e^{i\pi} = -1$, that very famous equation). We have $R^4 e^{4i\theta} = 2e^{i\pi}$, and $R = 2^{1/4}$ and $4\theta = \pi$ (modulo 2π). So $\theta \in \{\pi/4, 3\pi/4, 5\pi/4, 7\pi/4\}$. Observe that $2^{1/4}cis(\pi/4)$ and $2^{1/4}cis(7\pi/4)$ are conjugate. Since their sum is the splitting field S of our polynomial $a(x)$, it follows that $2(2^{1/4}$ is in S. It now follows that $2^{1/4}$ is in S, which implies that $cis(\pi/4) \in S$. So $(cis(\pi/4))^2 = i$ is in S. Of course $cis(\pi/4) = \sqrt{2}/2 + i\sqrt{2}/2$. Since $\sqrt{2} = (2^{1/4})^2$, $\sqrt{2} \in S$. Since $i \in S$, it follows that $cis(\pi/4) \in \mathbb{Q}(2^{1/4}, i)$.

   It now follows readily that $S = \mathbb{Q}(2^{1/4}, i)$ (since the right-most field contains all roots of $a(x) = x^4 + 2$ and, as we showed, S

contains $2^{1/4}$ and i.

What is $[S:\mathbb{Q}]$? We have $[S:\mathbb{Q}] = [\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}(2^{1/4})][\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = (2)(4)$ (since $i \notin \mathbb{Q}(2^{1/4})$ and $2^{1/4}$ is a root of the irreducible $x^4 - 2$, an irreducible polynomial over $\mathbb{Q}$.

(b) $b(x) = x^4 + x^2 + 1$:

Note that $b(x) = (x^2 + x + 1)(x^2 - x + 1)$, a pair of $\mathbb{Q}$-irreducible quadratic polynomials with roots $\{-\frac{1}{2} \pm \alpha\}$ and $\{\frac{1}{2} \pm \alpha\}$, where $\alpha = \frac{\sqrt{3}}{2}i$. It follows that the splitting field can be given by $\mathbb{Q}(\sqrt{3}i)$, and since α is a root of the irreducible $x^2 + 3$, the dimension of the s.f. over $\mathbb{Q}$ is 2.

4. Suppose $a \in Z_p$, with $a \neq 0$. Show $f(x) = x^p - x + a \in Z_p[x]$ is irreducible.

Observe that if b is a root of $f(x)$, then $f(b+1) = b^p + 1 - (b+1) + a = b^p + b + a = 0$. So $\{b, b+1, \ldots, b+(p-1)\}$ consist of p distinct roots, which means $f(x)$ is separable. Moreover, $b \notin Z_p$—if it was, $b + (-b) = 0$, which isn't the case since $a \neq 0$. (Note that $Z_p(b)$ is a splitting field for $f(x)$ since it contains all of $f(x)$'s roots, and no proper subfield could split $f(x)$.)

Consider $m_b(x)$, the minimal polynomial of b over Z_p. For $k \in \{1, \ldots, p-1\}$, let $m_b(x-k)$ is a monic polynomial having the same degree as $m_b(x)$, and having $b+k$ as a root. It follows readily that the minimal polymomials $\{m_{b+k}(x) : k = 0, 1, \ldots, p-1\}$ all have the same degree, and consist of that set consists of p distinct monic irreducible polynomials. Since $f(b+k) = 0$, it follows that $m_{b+k}(x)|p(x)$ for $k = 0, 1, \ldots, p-1$. But $Z_p[x]$ is a UFD, from which it follows that $f(x) = \Pi_{p>k\geq 0} m_{b+k}(x)$. However, $deg(f(x)) = p$ implies $m_{b+k}(x)$ are degree 1, and since $b+k$ is a root of $m_{b+k}(x)$, $b+k \in Z_p$, contradicting that Z_p contains any root of $f(x)$, completing the proof.

Interesting, useful fact.

Let F be a field, $t(x) \in F[x]$ a separable monic polynomial. As we know, there exists a splitting field of $t(x)$, an extension S/F. (So we're calling the s.f. S.)

Let $r_1, \ldots, r_k$ be the roots of $t(x)$, all contained in S, and let $m_1(x), m_k(x)$ be the minimal polynomials of r_i, for $i = 1, \ldots, k$. For each i, $t(r_i) = 0$; hence, $m_i(x)|t(x)$. Since $F[x]$ is a UFD, $m_1(x) \ldots m_k(x)|t(x)$. It could be that $m_i(x) = m_j(x)$, i.e. different roots have the same minimal polynomial. Assume that $m_1(x), \ldots, m_j(x)$ represent the distinct minimal polynomial is a under consideration. Since $F[x]$ is a UFD, $m_1(x) \ldots m_j(x)|t(x)$. But in S, the roots of $m_1(x) \ldots m_j(x)$ and those of $t(x)$ coincide. Hence the degree of $m_1(x) \ldots m_j(x)$ is the same as that of $t(x)$, from which it follows that $t(x) = m_1(x) \ldots m_j(x)$.

Fact of the week. If $t(x) \in F[x]$ is monic and separable, then in any extension T that splits $t(x)$, we have $t(x)$ is the product of the distinct minimal polynomials $m_b(x)$ over F, where the product ranges over the distinct roots of $t(x)$ in T and no $m_b(x)$ is allowed to occur more than once.