Solutions to Homework 9

1. Read §2 in Appendix 2 in Lang's *Algebra* (3rd edition). Find the place in his proof of Zorn's Lemma (pp. 881-884) where the axiom of choice is used. Write down where it is.

In the proof of Cor 2.4, he constructs $f : S \to S$. This requires the axiom of choice. More precisely, for all $x \in A$, define $A_x = \{y \in A \,|\, x < y\} \neq \emptyset$. It is clear that f is nothing other than an element in $\prod_{x\in A} A_x$, which is a non-empty set by the axiom of choice.

2. This exercise works out some splitting fields over $\mathbf{F}_p$'s.
(*i*) Prove that $f = X^3 - X + 1 \in \mathbf{F}_3[X]$ has splitting field $\mathbf{F}' = \mathbf{F}_3[y]/f(y)$ (factorize f into linears over this extension, say letting $\zeta \in \mathbf{F}'$ be the residue class of y).
(*ii*) Describe the splitting fields of $X^3 - 5$ over $\mathbf{F}_{11}$ and $\mathbf{F}_7$, and factor f over each.

(*i*) For ζ a root of f in a splitting field over $\mathbf{F}_3$, the relation $f(\zeta) = 0$ allows one to check that

$$(X - \zeta)(X - (\zeta + 1))(X - (\zeta - 1)) = f(X)$$

in $F[X]$. Thus, $\mathbf{F}_3(\zeta) \simeq \mathbf{F}_3[y]/f$ gives a 'description' of a splitting field of f over $\mathbf{F}_3$.
(*ii*) In $\mathbf{F}_{11}[X]$, we have $X^3 - 5 = (X-3)(X^2+3X-2)$, with the quadratic factor irreducible, so a splitting field is $\mathbf{F}_{11}[X]/(X^2+3X-2)$. In $\mathbf{F}_{13}[X]$, $X^3 - 5 = (X+5)(X+2)(X+6)$, so the splitting field is just $\mathbf{F}_{13}$. In $\mathbf{F}_7[X]$, $X^3 - 5$ is irreducible. Note that $\mathbf{F}_7$ has 3 cube roots of 1, namely 1, 2, and 4, so once we have one root r in a splitting field, the others are $2r$ and $4r$, so in $k = \mathbf{F}_7[T]/(T^3 - 5)$, with t denoting the image of T in k, we have $X^3 - 5 = (X - t)(X - 2t)(X - 4t)$. Thus, k is a splitting field for $X^3 - 5$ over $\mathbf{F}_7$.

3. Let k be a field with characteristic $p > 0$. Let $a \in k$ be an element which is not a pth power in k (e.g., $k = \mathbf{F}_p(T)$ and $a = T$). Show that $X^{p^n} - a \in k[X]$ is irreducible (hint: look at a splitting field over k and induct on n).

The case $n = 0$ is trivial. Now assume $n > 0$. Over a splitting field F of $f = X^{p^n} - a$, we have $f = (X - \alpha)^{p^n}$, where $\alpha^{p^n} = a$. Consider a factorization $f = gh$ in $k[X]$, in which we can assume g and h are monic without loss of generality. This must have the form $g = (X - \alpha)^i$ and $h = (X - \alpha)^j$ with $i + j = p^n$. Suppose $i > 0$. The second-highest term in g is $-i\alpha X^{i-1}$. If i is not divisible by p, then $\alpha \in k$, so $a = \alpha^{p^n} = (\alpha^{p^{n-1}})^p$ is a pth power in k (since $n > 0$), a contradiction. Thus, $i = pi'$ (even if $i = 0$) and similarly $j = pj'$. It follows that for $T = X^p$, we have $T^{p^{n-1}} - a = G(T)H(T)$ in $k[T]$ with $G = (T - \beta)^{i'}$ and $H = (T - \beta)^{j'}$ lying in $k[T]$ (where $\beta = \alpha^p$). By induction, $i' = 0$ or $j' = 0$, so $i = 0$ or $j = 0$.

4. Prove that 3 is prime in $\mathbf{Z}[i]$ (you may take for granted that $\mathbf{Z}[i]$ is a UFD), and deduce that $\mathbf{Z}[i]/3$ is a field of size 9. Give an explicit isomorphism between $\mathbf{F}_3[X]/(X^2 + X - 1)$ and $\mathbf{Z}[i]/3$. How many such isomorphisms are there?

If $3 = xy$ is a nontrivial factorization in $\mathbf{Z}[i]$, then multiplying each side by its complex conjugate gives $9 = (x\overline{x})(y\overline{y})$ where $x\overline{x} = a^2 + b^2 \in \mathbf{Z}$ for $x = a + bi$ and similarly for y. The positive integer $x\overline{x}$ cannot be 1 (as otherwise x would be a unit), and likewise for $y\overline{y}$, so by unique factorization in $\mathbf{Z}$ we get $x\overline{x} = 3$. But $a^2 + b^2 = 3$ does not have solutions in $\mathbf{Z}$. Thus, 3 is prime in the UFD $\mathbf{Z}[i]$, and hence $\mathbf{Z}[i]/3$ is a domain which is finite, and hence is a field. It clearly has size 9, since $a + bi \bmod 3$ is the same as specifying $a \bmod 3$ and $b \bmod 3$.
Define $k_1 = \mathbf{F}_3[X]/(X^2 + X + 1)$ and $k_2 = \mathbf{Z}[i]/3 \simeq \mathbf{F}_3[T]/(T^2 + 1)$. Both fields are finite with the same size and maps between fields are injective, so an isomorphism $k_1 \simeq k_2$ is the same thing as a ring map $k_1 \to k_2$. Such a map is the same thing as a solution to $x^2 + x + 1 = 0$ in k_2, so there are at most 2 such maps. In fact, $x = T + 1$ and $x = -T + 1$ are two such elements in k_2. So there are two such isomorphisms.

5. Let k be a finite field (e.g., $k = \mathbf{F}_p$ or $k = \mathbf{F}_p[X]/f$ with $f \in \mathbf{F}_p[X]$ irreducible). Let p denote the characteristic of k (note p is positive since k can't contain $\mathbf{Q}$).
(*i*) Show that $|k| = p^r$ for some positive integer r.
(*ii*) Let L/k be any extension field. Show that $k = \{x \in L \,|\, x^{p^r} = x\}$, so k is the *unique* subfield in L with size p^r. Moreover, show that for any $r \geq 1$, there exists a finite field with size p^r.

(*iii*) Prove that all finite fields with the same size are abstractly isomorphic!
(*iv*) Prove that a finite field with size q admits an injection into a finite field with size q' if and only if $q|q'$.

(*i*) Let $r = [k : \mathbf{F}_p]$ and choose an $\mathbf{F}_p$-basis for k.
(*ii*) Since $k^\times$ is a group of order $p^r - 1$, $x^{p^r-1} = 1$ for all non-zero $x \in k$. Thus, $x^{p^r} - x = 0$ for all $x \in k$. But the polynomial $T^{p^r} - T \in L[T]$ can have at most p^r zeros in L, so since $k \subseteq L$ already furnishes p^r such zeros, k is the set of all such zeros in L. This shows the uniqueness of k inside of L. Let F be a splitting field of $T^{p^r} - T$ over $\mathbf{F}_p$ and define $k = \{x \in F \mid x^{p^r} - x = 0\}$. It is easy to check that k is a subfield of F (and so in fact $k = F$!).

It remains to check that k has size p^r, which is to say that $f = T^{p^r} - T$ has p^r distinct roots in F. Equivalently, if $a \in F$ is a root of f (i.e., $T - a$ is a factor of f in $F[T]$), we want that $f(T + a)$ has a unique factor of T. But it is easy to compute that $f(T + a) = f(T)$, which clearly has a unique factor of T.
(*iii*) The previous part shows that a finite field with size p^r is the same as a splitting field over $\mathbf{F}_p$ of the polynomial $T^{p^r} - T$.
(*iv*) If k with size p^r is a subfield of k' with size $p^{r'}$, then $[k : \mathbf{F}_p]|[k' : \mathbf{F}_p]$, so $r|r'$. Conversely, if $r|r'$, then $T^{p^r} - T$ divides $T^{p^{r'}} - T$ in $\mathbf{F}_p[X]$ (why?), so a splitting field for the latter polynomial contains a splitting field for the former.