MATH 594. HOMEWORK 9 (DUE MARCH 26)

1. Read §2 in Appendix 2 in Lang's *Algebra* (3rd edition), a copy of which was handed out in class. 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.

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); recall that f is irreducible in $\mathbf{F}_3[X]$ by Exercise 6, HW 7.

(*ii*) Describe the splitting fields of $X^3 - 5$ over $\mathbf{F}_{11}$ and $\mathbf{F}_7$, and factor f over each.

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).

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?

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*) Show that a finite field with size p^r admits an injection into a finite field with size $p^{r'}$ if and only if $r|r'$ (note that by taking r' a non-trivial multiple of r, this shows that finite fields cannot be algebraically closed).

REMARK Due to this exercise, for any prime power $q = p^n$, there is an essentially unique finite field with size q, but the isomorphisms between finite fields with the same size are highly non-unique in general (unless $q = p$); cf. Exercise 4. Thus, one should usually not speak of 'the' finite field with size q, but merely 'a' finite field of with size q. However, if we are working inside of a fixed field F of characteristic p, then by (*ii*) it is legal to then speak of 'the' finite field of size q (understood to be inside of F), if it exists in F. We then often write $\mathbf{F}_q$ for this field. Many sloppy authors actually write $\mathbf{F}_q$ even if they are not working inside of a fixed field of characteristic p.