Nepal Algebra Project(NAP)
Central Department of Mathematics
Tribhuvan University,Kirtipur, Kathmandu,Nepal
Fields and Galois Theory-Homework 1
Course Instructor: Prof. Roger Wiegand and Prof. Sylvia Wiegand

Summary of NAP: Module -1, Lecture 2, 10 May, 2016

Discussion of irreducibility in $\mathbb{Z}[X]$ vs in $\mathbb{Q}[X]$:

Testing for irreducibility in $\mathbb{Z}[X]$ by checking irreducibility in $\mathbb{F}_p[X]$; proof of why it works, pitfalls of misinterpreting, why p must not divide leading coefficient. Explained what Milne means by "factors non-trivially" (not quite the same, over $\mathbb{Z}$, as being reducible). Examples, of a polynomial that can be shown to be irreducible by going mod 2 and of another polynomial, $X^4 - 10X^2 + 1$ in $\mathbb{Z}[X]$, that factors non-trivially modulo every prime, even though it is irreducible (proof of irreducibility assigned in Problem Set 1).

Finding a polynomial in $\mathbb{Z}[X]$ with $\sqrt{2} + \sqrt{3}$ as a root (the polynomial above, coincidentally).

Gauss' Lemma 1.13, proved with a more rigorous version of Milne's proof. (Choose appropriate positive rational multiples of $g(x)$ and $h(x)$ so as to minimize their integral product. then show that this minimal product must be 1.)

Vector spaces: Discussed how $F[X]$, and extension fields K of F are vector spaces over F.

Proposition 1.8: proved that for R a PID, gcd's exist and can be written as a combination of the generators. Discussed the Euclidean algorithm method of finding $d = \gcd(a, b)$ and r,s with $ra + sb = d$.

Stated and proved one case of the $\frac{2}{3}$ Lemma ("two-out of three lemma"): If $a, b, c, d \in R$, a commutative ring, with $d \neq 0$ and $a \pm b = c$, and two of a, b, c are multiplies of d, then so is the third.

Roger and Sylvia