MATH 123 SOLUTION SET 2

MD

Lang 1.7

Remark. This problem has the slight hitch of not being quite correct as stated: you need the property that $2xy = 0 \implies x = 0$ or $y = 0$ in F, which will fail in characteristic 2. Here's a counterexample from Steve: let $F = \mathbb{Z}_2[t]$ and let $\alpha = 1 + \sqrt{t}$, $\beta = \sqrt{t}$. Clearly, $F(\alpha) = F(\beta)$, but it is also clear that $t + 1 = c^2 t$ can't have solutions for $c \in F$.

Other than this hitch, here is how the problem could have gone without zero divisors:

1. Assume $F(\alpha) = F(\beta)$. Thus we can write $\alpha = c\beta + d$, since $\alpha \in F(\beta)$ and β has degree 2. This gives
$$a = c^2 b + 2cd\beta + d^2,$$
which must have $2cd\beta = 0$ to eliminate β. We know $\beta \neq 0$ since $\beta \notin F$, so here's where we make the jump and assume that $c = 0$ or $d = 0$. But c can't be 0 because that would force $\alpha \in F$, which isn't the case. So $d = 0$, which gives $a = c^2 b$.
2. Assume $\exists c \in F$ s.t. $a = c^2 b$. In the big containing field, $\alpha^2 - c^2\beta^2 = (\alpha + c\beta)(\alpha - c\beta)$, so it makes sense to write $\alpha = \pm c\beta$. So $\alpha \in F(\beta)$ and $F \subset F(\beta) \implies F(\alpha) \subset F(\beta)$. Since F is a field, though, we can invert c and write $\beta = \pm\frac{1}{c}\alpha$, so similarly we have $F(\beta) \subset F(\alpha)$. Taken together, these mean that $F(\alpha) = F(\beta)$.

Conclude that $F(\alpha) = F(\beta) \iff \exists c \in F$ s.t. $a = c^2 b$.

Lang 1.8

We're going to show that the degree of the field extension in question is either 2 or 1, then narrow it down to 2.

$\deg(\mathrm{irr}(\alpha, F)) = 2$ and $\mathrm{irr}(\alpha, F) \in F[x] \subset E_1[x]$, so $[E_1(\alpha) : E_1] \leq 2$ but $\alpha \notin E_1$ (else $\alpha \in E_1 \cap E_2 = F$, but it's not).

Conclude that the degree $[E_1(\alpha) : E_1]$ is exactly 2.

Lang 1.9

Here we'll begin with the standard way of breaking down such an extension:
$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$$
But $x^3 - 2$ is irreducible (by previous HW) so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Also we have that $\mathrm{irr}(\zeta, \mathbb{Q}) = x^2 + x + 1$ (shown on previous HW and **a useful fact**), thus ζ satisfies
$$\alpha^2(x^2 + x + 1) = (x\alpha)^2 + (x\alpha)\alpha + \alpha^2.$$
Thus, $(\zeta\alpha)^2 + (\zeta\alpha)\alpha + \alpha^2 = 0 \implies \beta^2 + \beta\alpha + \alpha^2 = 0$. So β satisfies $x^2 + \alpha x + \alpha^2 \in \mathbb{Q}(\alpha)[x]$. So the degree of β over $\mathbb{Q}(\alpha)$ is at most 2, and since $\beta \notin \mathbb{Q}(\alpha)$, it is exactly 2.

Remark. How do you show that $\beta \notin \mathbb{Q}(\alpha)$? Many people simply wanted to "observe" that $\mathbb{Q}(\alpha) \in \mathbb{R}$ or, equivalently, choose the real cube root of 2 for α or, also equivalently, choose an embedding of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ sending α to the real $\sqrt[3]{2}$, and claim that there was no loss of generality. Well, it's true - there isn't - but so far in this class we haven't really seen why. (So when Mike uses one of these mechanisms to simplify an explanation, it's because he knows it makes sense.) This will turn out to be defensible precisely because of the

Date: February 19, 1997.

symmetries of roots which we are in the process of learning about– the subject matter of Galois theory.

Lang 1.18

Let $m = \deg f$, $n = \deg g$. $(n, m) = 1$.

$$[F(\alpha,\beta):F] = [F(\alpha,\beta):F(\alpha)]\underbrace{[F(\alpha):F]}_{m} = [F(\alpha,\beta):F(\beta)]\underbrace{[F(\beta):F]}_{n}$$

This means that both n and m divide the total extension degree $[F(\alpha,\beta):F]$; since they are relatively prime, this means that $mn|[F(\alpha,\beta):F]$.

But note that $[F(\alpha,\beta):F(\alpha)] \leq [F(\beta):F] = n$ by the "translation lemma" (Lang Prop 1.5) so by tower multiplication, this means that $[F(\alpha,\beta):F] \leq nm$.

The combination of these 2 pieces of information yields that $[F(\alpha,\beta):F] = nm$ exactly. But then $[F(\alpha,\beta):F(\alpha)] = n$ so the irreducible polynomial for β over $F(\alpha)$ will have degree n. Since β satisfies g, which has that degree, g must be $\mathrm{irr}(\beta, F(\alpha))$, up to constant scaling. (Otherwise, the irreducible factor of g satisfied by β would contradict our findings.)

Lang 1.19

The polynomials $x^3 - 2$, $x^4 - 3$ are irreducible by Eisenstein on 2 and 3, respectively. Using the results of the last problem, we know that $x^4 - 3$ remains irreducible over $\mathbb{Q}(\alpha)$ since $(3, 4) = 1$. Thus

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}] = 3\cdot 4 = 12.$$

Lang 1.21

This problem simply seeks to make sure you're not spooked out by the finite field $F = \mathbb{Z}/2\mathbb{Z}$. If the cubic were reducible, it would have a linear factor– that is, a root in F. But the only elements of F are 0 and 1, and $f(0) = f(1) = 1$. Thus the cubic is irreducible, so $\deg \alpha = \deg f = 3$.

Lang 1.22

We can exhibit a polynomial in $K[x] = C(t)[x]$ which is satisfied by α, namely $f(x) = x^n - t$. It is irreducible by the handy generalized Eisenstein Criterion you can find in Lang on page 149... note that t being prime means, in this context, being a primitive irreducible. Since this irreducible polynomial has degree n, conclude that $[K(\alpha):K] = n$.