

PS 5 Solutions

Math 256 Section 31

May 5, 2005

31.22) If $b \neq 0$, then $a + bi \in \mathbb{C} \setminus \mathbb{R}$, so $[\mathbb{R}(a + bi) : \mathbb{R}] > 1$. Thus $[\mathbb{C} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}(a + bi)][\mathbb{R}(a + bi) : \mathbb{R}] = 2$ and so $[\mathbb{C} : \mathbb{R}(a + bi)] = 1$, so $\mathbb{C} = \mathbb{R}(a + bi)$.

31.32) If α is algebraic over \overline{F}_E , then $\overline{F}_E(\alpha)$ is algebraic over \overline{F}_E and by definition, \overline{F}_E is algebraic over F . By Exercise 31, then $\overline{F}_E(\alpha)$ is algebraic over F , so α is algebraic over F . But then $\alpha \in \overline{F}_E$ contrary to hypothesis. Thus α is transcendental over \overline{F}_E .

31.34) Let $\alpha \in E$ and let $p(x) = \text{irr}(\alpha, F)$ have degree n . Now $p(x)$ factors into $(x - \alpha_1) \cdots (x - \alpha_n)$ in $\overline{F}_E[x]$. Because by hypothesis all zeros of $p(x)$ in \overline{F} are also in E , we see that this same factorization is also valid in $E[x]$. Hence $p(\alpha) = (\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0$, so $\alpha = \alpha_i$ for some i . This shows that $F \leq E \leq \overline{F}$. Because by definition \overline{F} contains only elements that are algebraic over F and E contains all of these, we see that $E = \overline{F}$ and is therefore algebraically closed.

31.38) If R contains no nontrivial proper ideals, then $\{0\}$ is the only proper ideal, and it is maximal, and is contained in itself, so we are done.

Suppose R contains a nontrivial proper ideal N which of course does not contain the unity 1 of R . The set S of ideals of R that do not contain 1 is partially ordered by inclusion. Let $T = \{N_i \mid i \in I\}$ be a chain in S . Want to show that $U = \bigcup_{i \in I} N_i$ is an element of S that is an upper bound of T . Let $x, y \in U$, then $x \in N_j$ and $y \in N_k$ for some $j, k \in I$. Because T is a chain, one of these ideals is contained in the other, say $N_j \subset N_k$. Then $x, y \in N_k$ which is an ideal, so for all $r \in R$, we see that $x \pm y, 0, rx$, and xr are all in N_k and hence in U . Thus U is an ideal. Clearly $N_i \subset U$ for all $i \in I$, and 1 is not in U because it is not in any N_i . Thus $U \in S$ and is an upper bound for T , so we may apply Zorn's Lemma.

So, let M be a maximal element of S . $M \in S$ so M is an ideal of R , and does not contain 1 so $M \neq R$. Suppose that L is a proper ideal of R such that $M \subset L \subset R$. $1 \notin L$, so $L \in S$, so $M = L$ because M is maximal in S under inclusion. Thus M is a maximal ideal of R .

33.9) Both polynomials are irreducible over \mathbb{Z}_2 , both $\mathbb{Z}_2(\alpha)$ and $\mathbb{Z}_2(\beta)$ are extensions of \mathbb{Z}_2 of degree 3 and thus are subfields of $\overline{\mathbb{Z}_2}$ containing $2^3 = 8$ elements. Theorem 33.3 gives that both of these fields must consist precisely of the zeros in $\overline{\mathbb{Z}_2}$ of the polynomial $x^8 - x$ and so they are the same.

33.10) Let $p(x)$ be irreducible of degree m in $\mathbb{Z}_p[x]$. Let K be the finite extension of \mathbb{Z}_p obtained by adjoining all the zeros of $p(x)$ in $\overline{\mathbb{Z}_p}$. Then K is a finite field of order p^n for some positive n and consists precisely of all zeros of $x^{p^n} - x$ in $\overline{\mathbb{Z}_p}$. $p(x)$ factors into linear factors in $K[x]$ and these linear factors are among the linear factors of $x^{p^n} - x$ in $K[x]$. Thus, $p(x)$ is a divisor of $x^{p^n} - x$.

33.11) $\alpha \in F$, so $\mathbb{Z}_p(\alpha) \subset F$, but α is a generator of the multiplicative group F^* , we have that $\mathbb{Z}_p(\alpha) = F$. $|F| = p^n$, so the degree of α over \mathbb{Z}_p is n .