

PS 7 Solutions

Math 256 Section 31

May 29, 2005

32.10) Using a straightedge and compass we can construct points that are the intersections of lines and circles through already constructed points. This amounts to solving linear and quadratic equations. To construct an angle of 20° , we need to construct a line segment of length $\cos 20^\circ$, but $\cos 20^\circ$ is the solution of a cubic and not a quadratic, so we cannot construct such an angle.

33.12) Let \overline{F} be an algebraic closure of F , a field of p^n elements. Let m be a divisor of n , so $n = mq$. If $\alpha \in \overline{F}$ such that α^{p^m} then $\alpha^{p^n} = \alpha^{p^{mq}} = (\alpha^{p^m})^{p^{m(q-1)}} = \alpha^{p^{m(q-1)}} = \dots = \alpha^{p^m} = \alpha$. All such α form the unique subfield of \overline{F} of order p^m . Also, every such α is a zero of $x^{p^n} - x$ and so is in F . So F contains a unique subfield of order p^m .

33.13) Let F be an extension of \mathbb{Z}_p of degree n . Each $\alpha \in F$ is algebraic over \mathbb{Z}_p , so let d be the degree of α over \mathbb{Z}_p (so that α satisfies a monic irreducible polynomial of degree d). We have $n = [F : \mathbb{Z}_p] = [F : \mathbb{Z}_p(\alpha)][\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = [F : \mathbb{Z}_p(\alpha)]d$, so d divides n . Now, let β be a zero of a monic irreducible polynomial of degree d dividing n . Then $\mathbb{Z}_p(\beta)$ has order p^d , so by problem 12, $\beta \in F$. Thus, the elements of F are exactly the zeros of all irreducible polynomials in $\mathbb{Z}_p[x]$ of some degree d dividing n . Also, the elements of F are exactly the zeros of $x^{p^n} - x$. Let $X = \{g \in \mathbb{Z}_p[x] \mid \deg g \text{ divides } n\}$. By factoring in F and then grouping the zeros of a given irreducible we see $x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha) = \prod_{g \in X} g$.

33.14) a) $x^2 \equiv a \pmod{p}$ has a solution in \mathbb{Z} iff $x^2 = b$ has a zero in \mathbb{Z}_p , where $b = a \pmod{p}$. Now \mathbb{Z}_p^* is cyclic of order $p - 1$. The elements of a cyclic group that are squares are exactly the elements that are even powers of a generator, and these are exactly the elements b satisfying $b^{\frac{p-1}{2}} = 1$ and this implies the result.

b) We know that $x^2 - 6$ is irreducible in $\mathbb{Z}_{17}[x]$ iff it has no zeros in \mathbb{Z}_{17} iff $6 \neq b^2$ for any $b \in \mathbb{Z}_{17}$. $6^{\frac{17-1}{2}} = 6^8 = (6^2)^4 \equiv 2^4 = 16 \not\equiv 1 \pmod{p}$, so a) gives that there are no such b . Thus, $x^2 - 6$ is irreducible.