Mathematics GU4042
Introduction to Modern Algebra II

Answers to Practice Final

May 9, 2017

1. A finite separable field extension is simple (i.e. has a primitive element).

2. Field $\Rightarrow$ Euclidean domain $\Rightarrow$ principal ideal domain $\Rightarrow$ unique factorization domain $\Rightarrow$ integral domain $\Rightarrow$ ring.

3. Consider $g : \mathbb{F}_q \setminus 0 \to \mathbb{F}_q \setminus 0$ given by $g(a) = a^2$. If $b \in g(\mathbb{F}_q \setminus 0)$, say $b = g(a)$, then $b = g(-a)$ too, and $a \neq -a$ since $a \neq 0$ and char $\mathbb{F}_q \neq 2$ imply $2a \neq 0$. However, there are at most 2 roots of $x^2 - b$. Hence $\#g^{-1}(b) = 2$. So the number of nonzero squares $= \#g(\mathbb{F}_q \setminus 0) = \#(\mathbb{F}_q \setminus 0)/2$.

4. False. These two rings are isomorphic to $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\sqrt{3}]$ respectively, by the first isomorphism theorem. If there were an isomorphism $\psi : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}[\sqrt{3}]$, then $\psi(\sqrt{-3}) = a + b\sqrt{3}$ for some $a, b \in \mathbb{Z}$, and then $-3 = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}$, so $2ab = 0$ and $-3 = a^2 + 3b^2$, which is impossible.

5. (a) Three. There are three cube roots of -7, say r_1, r_2, r_3, with only r_1 real. Hence $E = \mathbb{Q}(r_1, r_2, r_3) \neq \mathbb{Q}(r_1)$ since the latter is $\subset \mathbb{R}$. So $[E : \mathbb{Q}] = [E : \mathbb{Q}(r_1)][\mathbb{Q}(r_1) : \mathbb{Q}] > [\mathbb{Q}(r_1) : \mathbb{Q}] = 3$. Hence $r_i \notin \mathbb{Q}(r_j)$ for $i \neq j$, since if it were, the third root $r_k = r_i^2/r_j \in \mathbb{Q}(r_j)$ too and hence $E = \mathbb{Q}(r_j)$, so $[E : \mathbb{Q}] = [\mathbb{Q}(r_j) : \mathbb{Q}] = 3$. So the three $\mathbb{Q}(r_j)$ are all different. But each is isomorphic to $\mathbb{Q}[r_j]$, hence to $\mathbb{Q}[x]/(x^3 + 7)$ by the first isomorphism theorem.

(b) One, the real field $\mathbb{Q}(r_1)$ discussed above.

6. (a) $x^7 + 3x^4 + 18x^2 - 21$ irreducible by Eisenstein, since 3 divides $3, 18, 21$ but 3^2 does not divide 21; (b) $2x(x+1)^3$ by the binomial theorem; (c) $(x-1)(x+1)(x^2+x+1)(x^2-x+1)$ is the decomposition into cyclotomic factors, and cyclotomic polynomials are all irreducible.

7. Let ζ be a primitive 7th root of unity. Then we know $\mathbb{Q}(\zeta)$ has Galois group $\mathbb{Z}_7^\times \cong \mathbb{Z}_6$. The subgroup H generated by complex conjugation σ is normal of order 2. Clearly $\zeta + \zeta^{-1}$ is real, positive, and invariant under σ, but it is not rational (e.g. since one can check a generator for the Galois group takes it to $\zeta^3 + \zeta^4$, which is real and negative). So it generates $\mathbb{Q}(\zeta)^H$, which by the FTGT is Galois of degree 3 over $\mathbb{Q}$. Its powers are 1, $\zeta + \zeta^{-1}$, $\zeta^2 + 2 + \zeta^{-2}$, $\zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}$, so because the 7th roots of unity add to 0, it is a root of $f(x) = x^3 + x^2 - 2x - 1$, which is therefore the minimal polynomial.

8. No such field exists, for if it did, by the primitive element theorem it would be $\cong \mathbb{R}[x]/(f)$ for some irreducible $f \in \mathbb{R}[x]$ of degree 5. But we proved in A3#5 (assuming the Fundamental Theorem of Algebra) that the only irreducible polynomials in $\mathbb{R}[x]$ are of degree 1 or 2.

Alternative (not assuming the Fundamental Theorem of Algebra): No such field exists, for if it did, the minimal polynomial over $\mathbb{R}$ of any element not in $\mathbb{R}$ would be an irreducible polynomial of degree 5 over $\mathbb{R}$. This contradicts Lemma 1 from the last lecture, which asserts that every polynomial of odd degree over $\mathbb{R}$ has a root.

9. (a) If ϕ is a homomorphism and a is idempotent, then $\phi(a) = \phi(a^2) = \phi(a)^2$ is idempotent. (b) There are two, mapping (a, b) to a and b respectively. It is easy to check that these are homomorphisms. On the other hand, since $(1, 0)$ and $(0, 1)$ are idempotents, by (a) any

homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ takes them to 0 or 1. We must have $\phi(1,1) = 1$ since $(1,1)$ is the multiplicative identity. Hence $\phi(1,0) = 1$ and $\phi(0,1) = 0$ or vice versa. Then $\phi(a,b) = a\phi(1,0) + b\phi(0,1) = a$ or b.

10. (a) $145 = 5 \cdot 29 = (2^2+1^2)(5^2+2^2) = (2+i)(2-i)(5+2i)(5-2i)$ and we proved in A5#7 that these are irreducible. (b) If $145 = a^2 + b^2$, then $145 = (a+bi)(a-bi)$, and since $\mathbb{Z}[i]$ is a ufd, $a+bi$ must be a product of factors from (a), and $a-bi$ a product of the conjugate factors, up to units ± 1, $\pm i$. These units only reverse the order of the squares, so the only possibilities are $a+bi = (2+i)(5+2i) = 8+9i$ leading to $145 = 8^2+9^2$ and $a+bi = (2+i)(5-2i) = 12+i$ leading to $145 = 12^2 + 1^2$, and their conjugates which lead to the same sums.

11. By the Chinese remainder theorem for rings, $\mathbb{Z}_{24} \cong \mathbb{Z}_3 \times \mathbb{Z}_8$ as rings, so $\mathbb{Z}_{24}^\times \cong (\mathbb{Z}_3 \times \mathbb{Z}_8)^\times = \mathbb{Z}_3^\times \times \mathbb{Z}_8^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2^2$. So not cyclic.

12. (a) $0 \subset \mathbb{Q}[x]$ is prime but not maximal, for $\mathbb{Q}[x]/0 \cong \mathbb{Q}[x]$ is an integral domain but not a field. (b) This is impossible: if I is maximal, then R/I is a field, hence an integral domain, so I is prime.

13. (a) If $f = 0$, then $f(a) = 0$ for all a by definition. Conversely, if $f(a) = 0$ for all a, then $x - a \mid f(x)$ for all a; if $f \neq 0$, these would constitute infinitely many irreducible factors, which is impossible since $F[x]$ is a ufd. (b) There is some constant $b \in F$ such that $0 \neq f(x,b) \in F[x]$. For if not, and $f(x,b) = 0$, then using the division algorithm in $F[x,y] = F[x][y]$, we find that $(y-b) \mid f(x,y)$ for all b, which again is impossible since $F[x,y]$ is a ufd. If $0 \neq f(x,b)$ as a polynomial, then it has finitely many roots, so there exist only finitely many $a \in F$ such that $f(a,b) = 0$ for this b, let alone for all b.

14. The splitting field of any $f = \prod f_i^{n_i}$ over $\mathbb{Q}$ is the same as the splitting field of $\bar{f} = \prod f_i$ over $\mathbb{Q}$, the product of the same irreducible factors without repeats. Since $\bar{f}$ is separable, E is Galois over $\mathbb{Q}$. Any field of characteristic zero contains $\mathbb{Q}$, so all subfields of E contain $\mathbb{Q}$. By the Galois correspondence, they are in bijection with the subgroups of the finite group Gal $E/\mathbb{Q}$, which are finite in number since the subsets are.