Short proofs to practice for the final

The following problems are roughly in reverse chronological order. You should be able to do each in one handwritten page or less (usually half a page should be plenty). I recommend that you first try them with no resources and then go back and use your book for any you couldn't do the first time. If one seems to be much harder than expected, let me know so I can give a hint (or revise the problem if I made it too hard).

1. We know that the set of functions $F = \{f : \mathbb{R} \to \mathbb{R}\}$ is a ring under (pointwise) addition and multiplication, and we have seen several subrings and ideals. We have also seen some *groups* of functions where the binary operation is function composition (e.g. permutations). Prove that the set F above is NOT a ring under addition and composition. (Hint: rings need to satisfy distributive laws.)

2. Suppose E is an extension field of a field F, and $\alpha \in E$ is algebraic over F. If $\beta \in F(\alpha)$, prove that $F(\beta)$ is a subfield of $F(\alpha)$. (Hint: if you show that you can write all elements in $F(\beta)$ as linear combinations of the small powers of α, then you'll be done. You can definitely write β this way, since you know it's in $F(\alpha)$ – how do you deal with the rest of the elements?)

3. Suppose F is a field of characteristic p, where p is an odd prime. We showed in HW that there must exist an extension field E of degree 2 over F. Can we use a nearly identical proof to show that there exists an extension field of degree 3 over F? What about degree 4?

4. Suppose E is an extension field of F. If $\alpha \in E$ is algebraic over F and $\beta \in F(\alpha)$, prove that $deg(\beta, F)$ divides $deg(\alpha, F)$.

5. Suppose E is a finite extension of a field F. Let $p(x) \in F[x]$ be a polynomial which is irreducible over F. Prove that if E contains a zero of $p(x)$, then the degree of $p(x)$ divides $[E : F]$. Show that this is not necessarily true if $p(x)$ is not irreducible.

6. Suppose E is a finite extension of a field F and $[E : F]$ is a prime number. Prove that $E = F(\alpha)$ for every $\alpha \in E$ which is not already in F.

7. Prove that the extensions $\mathbb{Q}(\sqrt{5} + \sqrt{2})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{10})$ of $\mathbb{Q}$ are equal.

8. Prove that there exists a field with exactly 8 elements.

9. Assuming that π is transcendental over $\mathbb{Q}$, prove that π^3 is also transcendental over $\mathbb{Q}$.

10. Describe how to construct a vector space of dimension 4 over $\mathbb{Q}$. (Hint: start by finding an appropriate irreducible polynomial).

11. Let $q(x)$ be an irreducible quadratic in $\mathbb{Z}_5[x]$. Prove that if the cosets $ax+b+\langle q(x)\rangle$ and $cx+d+\langle q(x)\rangle$ are equal in $\mathbb{Z}_5[x]/\langle q(x)\rangle$, then $a = c$ and $b = d$ in $\mathbb{Z}_5$.

12. Suppose A and B are ideals of a ring R. Let $A + B = \{a + b : a \in A, b \in B\}$ (this is standard notation, not something I made up). Prove that $A + B$ is an ideal of R.

13. Suppose R is a ring with unity and I is an ideal of R. If I contains a unit of R, prove that $I = R$.

14. Let $\phi : R \to R'$ be a ring homomorphism. Prove that if S is a subring of R, then $\phi(S)$ is a subring of R'.

15. Let $\phi : R \to R'$ be a ring homomorphism. Prove that if I' is an ideal of R', then $I = \phi^{-1}(I')$ is an ideal of R.

16. Suppose k is an arbitrary element of $\mathbb{Z}_p$. Prove that the polynomial $x^p - k \in \mathbb{Z}_p[x]$ is reducible.

17. Prove using the definitions that x is neither a unit nor a zero divisor in $\mathbb{Z}[x]$.

18. State and prove Fermat's Little Theorem. (Hint: think about the multiplicative group of units of $\mathbb{Z}_p$).

19. Let p and q be primes. Find all elements of $\mathbb{Z}_p \times \mathbb{Z}_q$ which are their own multiplicative inverses (i.e. solutions to the equation $x^2 - 1 = 0$), and justify your answer.

20. Suppose R is a ring with unity. If R has finite characteristic n and n is not prime, prove (from definitions) that R has zero divisors.

21. Prove that the matrix ring $M_2(\mathbb{Z}_3)$ is not an integral domain in two ways – a) show it is not commutative, b) show it has zero divisors.

22. Suppose R is a ring with no zero divisors, and $a, b, c \in R$. Prove the left cancellation law holds, i.e., if $ab = ac$, then $b = c$.

23. Find a nontrivial ring homomorphism whose kernel is isomorphic to $\mathbb{Z}$. (I.e. don't pick the only map $\mathbb{Z} \to \{0\}$.)

24. Suppose S and T are subrings of a ring R. Prove that $S \cap T$ is a subring of R. What if S and T are ideals – is $S \cap T$ also an ideal?

25. Determine (with proof) the isomorphism type of the quotient group $\mathbb{Z}_6 \times \mathbb{Z}_8 / \langle (0, 2) \rangle$, using the FTFGAG.

26. Determine (with proof) the isomorphism type of the quotient group $\mathbb{Z}_\times \mathbb{Z} / \langle (2, 0), (0, 2) \rangle$, using the FTFGAG.

27. Determine (with proof) the isomorphism type of the quotient group $\mathbb{Z} \times \mathbb{Z} / \langle (1, 1) \rangle$, using the FTFGAG.

See the midterm and practice midterm for more practice on earlier material.