Cf. 7.3.22. Let R be a ring, C be a subset of R, and $A = \mathrm{Ann}(C)$.

5pt (a) Prove that A is a left ideal in R.

Solution. $(A - A)C \subseteq AC - AC = 0$ and $(RA)C = R(AC) = 0$, so $A - A, RA \subseteq A$.

5pt (b) *If C is a left ideal of R, prove that A is a two-sided ideal.*

Solution. $(AR)C = A(RC) \subseteq AC = 0$, so $AR \subseteq A$, thus A is a right ideal as well.

5pt **7.3.20.** (a) *If I is a left ideal in a ring R and S is a subring of R, prove that $I \cap S$ is a left ideal in S.*

Solution. This is a special case of the fact that the preimage of any ideal under a homomorphism of rings is an ideal: $I \cap S = \varphi^{-1}(I)$ where φ is the imbedding $S \longrightarrow R$: $\varphi(x) = x$, $x \in S$. Or directly: $I \cap S$ is a subgroup of S under addition, and for any $s \in S$, $s(I \cap S) \subseteq sI \cap sS \subseteq I \cap S$.

5pt (b) *Show by example that not every left ideal of a subring S of a ring R needs to be of the form $I \cap S$ for some left ideal I of R.*

Solution. Consider $\mathbb{Z}$ as a subring of the ring (the field) $\mathbb{Q}$. $\mathbb{Q}$ has no ideals, except 0 and itself, but $\mathbb{Z}$ has many ideals.

5pt **7.4.6.** *Prove that a unital ring R is a division ring iff it has no nontrivial ($\neq 0, R$) left ideals.*

Solution. R is a division ring iff all its nonzero elements have left inverses. If R possesses a nonzero element a that doesn't have a left inverse, then Ra is a nontrivial left ideal. ($Ra \neq 0$ since $Ra \ni a$, and $Ra \neq R$ since $Ra \not\ni 1$.)

Conversely, if R has a nontrivial left ideal I, then any nonzero $a \in I$ has no left inverse. (If $b \in R$ is such that $ba = 1$, then $1 \in I$, so $I = R$.)

7.4.15. *Let x^2+x+1 be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and let $\overline{E} = E/(g)$ where $g = x^2+x+1$. For $f \in E$, let $\overline{f}$ be the image of f in $\overline{E}$.*

5pt (a) *Prove that $\overline{E} = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$.*

Solution. In $\overline{E}$, $\overline{x}^2 = -\overline{x} - \overline{1} = \overline{x} + \overline{1}$, so $\overline{x}^3 = (\overline{x} + \overline{1})\overline{x} = \overline{x}^2 + \overline{x} = \overline{x} + \overline{1} + \overline{x} = \overline{1}$, and by induction on the degree, every element of $\overline{E}$ can be written in the form $a\overline{x} + b$ for some $a, b \in \mathbb{Z}_2$, that is, $\overline{E} = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$, No two of the polynomials $0, 1, x, x+1$ are equal modulo g, so $\overline{E}$ has exactly 4 elements.

5pt (b) *Write the 4×4 addition table for $\overline{E}$ and deduce that $(\overline{E}, +) \cong V_4$.*

Solution.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

So, $\overline{E}$ under addition is a group with 4 elements in which every element has order 2; hence, under addition, $\overline{E} \cong V_4$.

5pt (c) *Write the 4×4 multiplication table for $\overline{E}$ and deduce that $(\overline{E}^*, \cdot) \cong \mathbb{Z}_3$. Deduce that $\overline{E}$ is a field.*

Solution. Since $x^2 = -x - 1 = x + 1$, $x(x+1) = x^2 + x = 1$, and $(x+1)^2 = x^2 + 2x + 1 = x$, we have

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Under multiplication, $\overline{E}$ is commutative and all nonzero elements of $\overline{E}$ are invertible (every row contains 1), hence, $\overline{E}$ is a field. The multiplicative group $\overline{E}^*$ has 3 elements, so it is isomorphic to $\mathbb{Z}_3$. ($\overline{E}^*$ is generated by x: $x^2 = x + 1$ and $x^3 = 1$.)

A1. *Let I, J, L be ideals in R. Prove that*

2pt (a) *if $I \mid J \mid L$ then $I \mid L$;*

Solution. If $L \subseteq J \subseteq I$, then $L \subseteq I$.

2pt (b) *if $I \mid J$ and $I \mid L$ then $I \mid \gcd(J, L)$;*

Solution. If $J, L \subseteq I$, then $J + L \subseteq I$ since $J + L$ is the minimal ideal containing J and L.

2pt (c) *if $I \mid L$ and $J \mid L$, then $\operatorname{lcm}(I, J) \mid L$;*

Solution. If $L \subseteq I, J$, then $L \subseteq I \cap J$.

5pt (d) *$IJ \mid \gcd(I, J) \operatorname{lcm}(I, J)$.*

Solution. The ideal $(I + J)(I \cap J)$ is generated by elements of the form $a = (b + c)d = bd + cd$ where $b \in I$, $c \in J$, and $d \in I \cap J$. Since $bd \in IJ$ and $cd \in JI = IJ$, we have $a \in IJ$.

5pt (e) *In the ring $\mathbb{Z}[x]$ (of polynomials with integer coefficients) let $I = (4)$ and $J = (2x)$. Prove that $IJ \neq \gcd(I, J) \operatorname{lcm}(I, J)$.*

Solution. We have $IJ = (8x)$, $I + J = (4, 2x)$, $I \cap J = (4x)$, and $(I + J)(I \cap J) = (16x, 8x^2)$. The polynomial $8x$ is contained in IJ but is not contained in $L = (16x, 8x^2)$ (since every nonzero element of L has form $16a_1x + 8a_2x^2 + \cdots + 8a_nx^n$ for some $a_1, \ldots, a_n \in \mathbb{Z}$).

Cf. 7.4.13. *Let R be a commutative unital rings and S be a subring of R.*

5pt (a) *If P is a prime ideal in R, prove that $P \cap S$ is either S or a prime ideal in S.*

Solution. Under the embedding $S \longrightarrow R$, $S \cap P$ is the preimage of P, and so, is either S or a prime ideal of S.

Or directly: for any $a, b \in S$, if $ab \in P$ then $a \in P$ or $b \in P$, so $a \in S \cap P$ or $b \in S \cap P$.

5pt (b) *Give an example of a ring R with a subring S and a maximal ideal M such that $M \cap S$ is neither S nor a maximal ideal of S.*

Solution. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, 0 is a maximal ideal in $\mathbb{Q}$, but $0 = 0 \cap \mathbb{Z}$ is not a maximal ideal in $\mathbb{Z}$.

7.4.33. *Let R be the ring $C([0, 1])$ of continuous functions $f : [0, 1] \longrightarrow \mathbb{R}$, and for each $c \in [0, 1]$ let $M_c = \{f \in R \mid f(c) = 0\}$.*

10pt (a) *Prove that if M is a maximal ideal in R then $M = M_c$ for some $c \in [0, 1]$.*

Solution. Assume that for every $c \in [0, 1]$ there is $f_c \in M$ such that $f_c(c) \neq 0$. Since f_c are continuous, for every $c \in C$, there is an open interval U_c containing c such that $f_c(x) \neq 0$ for all $x \in U_c$. The intervals U_c form an open cover of $[0, 1]$, so there are points $c_1, \ldots, c_n \in [0, 1]$ such that $\bigcup_{i=1}^n U_i = [0, 1]$. Then the function $f = f_1^2 + \ldots + f_n^2 \in M$ is positive on $[0, 1]$, and so, is a unit in R, so that $M = (1)$.

Hence, there is $c \in [0, 1]$ such that $f(c) = 0$ for all $c \in [0, 1]$. Then $M \subseteq M_c$; but since M is maximal, $M = M_c$.

10pt (d) *Prove that, for $c \in [0, 1]$, M_c is not finitely generated.*

Solution. Let $f_1, \ldots, f_n \in M_c$; we need to show that $M_c \neq (f_1, \ldots, f_n)$. Put $f = |f_1| + \cdots + |f_n|$, then $f(c) = 0$ and $f(x) > 0$ for all $x \neq c$, so $\sqrt{f} \in M_c$ with $\sqrt{f(x)} > 0$ for all $x \neq c$. Let $h_1, \ldots, h_n \in R$, and let $C = \max\{\sup |h_1|, \ldots, \sup |h_n|\}$; then for $g = h_1f_1 + \cdots + h_nf_n$ we have $|g| \leq C|f|$, so $|g|/\sqrt{f} \leq C\sqrt{f}$, and $(g/\sqrt{f})(x) \longrightarrow 0$ as $x \longrightarrow c$. Hence, $\sqrt{f} \neq g$, and so, $\sqrt{f} \notin (f_1, \ldots, f_n)$.