Solutions Review Multiple Choice

---

1. Consider the ring $R = \mathbb{Z}[i\sqrt{2}, \frac{1}{2}]$. Which of the following is a subring of R?

(a) $2\mathbb{Z}$

(b) $\mathbb{Z}[i]$

(c) $\{a \cdot i\sqrt{2} \mid a \in \mathbb{Z}\}$

(d) $\mathbb{Z}[\frac{i}{\sqrt{2}}]$

Solution: The only correct answer is (d): this follows from $\frac{i}{\sqrt{2}} = i\sqrt{2} \cdot \frac{1}{2}$. In fact we have $R = \mathbb{Z}[\frac{i}{\sqrt{2}}]$ since $i\sqrt{2} = \frac{i}{\sqrt{2}} \cdot 2$ and $\frac{1}{2} = -\left(\frac{i}{\sqrt{2}}\right)$.

For part (a), note that the subset does not contain 1.

The elements of R can all be written in the form $a+b(i\sqrt{2})$, with $a, b \in \frac{1}{2}\mathbb{Z}$. One sees directly that i cannot be written in this form, so part (b) is false.

For part (c), note that the subset is not closed under multiplication and does not contain 1.

2. Let $L : K$ be a finite extension of fields. Which of the following assertions are correct:

(a) If the characteristic of K is zero, then $L : K$ is normal.

(b) If the characteristic of K is zero, then $L : K$ is separable.

(c) If $L : K$ is normal, then $L : K$ is a Galois extension.

(d) If the characteristic of K is positive, then $L : K$ is normal if and only if it is separable.

Solution: Part (a) is not correct: as a counterexample take $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$; it is not normal.

Part (b) is correct: see lecture notes

Part (c) is not correct if $L : K$ is not separable; counterexample $\mathbb{F}_p(T^{1/p}) : \mathbb{F}_p(T)$.

Part (d) is not correct (counterexample: $\mathbb{F}_p(T^{1/p}) : \mathbb{F}_p(T)$ is normal but not separable).

3. Let K be a field, $\bar{K}$ an algebraic closure of K and $P \in K[X]$ a non-constant polynomial. Let $L \subset \bar{K}$ denote the splitting field of P in $\bar{K}$. Which of the following assertions are correct:

(a) The extension $L : K$ is a normal extension.

(b) If $x \in \bar{K}$ is a root of P, then $L = K(x)$.

(c) The extension $L : K$ is a Galois extension.

(d) If the polynomial P is irreducible, then $L : K$ is a Galois extension.

(e) If the characteristic of K is zero, then $L : K$ is a Galois extension.

Solution: Part (a) is correct (one of basic examples of a normal extension).

Part (b) is not correct, because a single root of P might not be enough (counterexample: $K = \mathbb{Q}$, $P = X^3 - 2$; then $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of P).

Part (c) is not always correct (only if P is separable; counterexample is $K = \mathbb{F}_p(T)$, $P = X^p - T$).

Part (d) is not always correct (only if P is separable; same counterexample).

Part (e) is correct (because $L : K$ is always separable in that case).

4. Let K be a field, $\bar{K}$ an algebraic closure of K and $L \subset \bar{K}$ a finite extension of K such that $L : K$ is a Galois extension. Let $K \subset E \subset L$ be an intermediate extension. Which of the following assertions are correct:

(a) The extension $L : E$ is a Galois extension.

(b) The extension $E : K$ is a normal extension.

(c) The extension $E : K$ is a separable extension.

Solution: Part (a) is correct (basic result from Galois correspondance)

Part (b) is not correct (counterexample: $K = \mathbb{Q}$, L splitting field of $X^3 - 2$, $E = \mathbb{Q}(\sqrt[3]{2})$; the $E : \mathbb{Q}$ is not normal).

Part (c) is correct (subextensions of separable extensions are separable, as follows for instance from the characterization using separability of minimal polynomials).

5. Let K be a field, $\bar{K}$ an algebraic closure of K and $L \subset \bar{K}$ a finite extension of K such that $L : K$ is a Galois extension, and let G be its Galois group. Which of the following assertions are correct:

(a) For any subgroup H of G, the intermediate extension $E = L^H$ is a normal extension of K.

(b) Two subgroups H_1 and H_2 of G are equal if and only if $L^{H_1} = L^{H_2}$.

(c) Any subgroup H of G is the Galois group of some extension $E : K$ for some $E \subset L$.

(d) Any subgroup H of G is the Galois group of some extension $L : E$ for some $E \subset L$.

Solution: Part (a) is not correct ($E = L^H$ is normal over K if and only if H is a normal subgroup of K)

Part (b) is correct (injectivity of the map $H \mapsto L^H$ in the Galois correspondance)

Part (c) is not correct (counterexample: if $G = S_3$ is the symmetric group and H is generated by a cycle of length 3, so that H has order 3, then an intermediate E with $\mathrm{Gal}(E : K) = H$ would correspond to a normal subgroup $K < G$ with $[S_3 : K] = [L : E] = 2$, but one can see easily that there is no normal subgroup of order 2 in S_3)

Part (d) is correct (Galois correspondance: one can take $E = L^H$ since $H = \mathrm{Gal}(L : L^H)$)

6. Let K be a field, $\bar{K}$ an algebraic closure of K and $L \subset \bar{K}$ a finite extension of K such that $L : K$ is a Galois extension, and let G be its Galois group. Let $x \in L$ be given and $\sigma_0 \in G$ a non-trivial element. Which of the following assertions are correct:

(a) If $\sigma_0(x) = x$, then $x \in K$.

(b) If G is cyclic and $\sigma_0(x) = x$, then $x \in K$.

(c) The element

$$\sum_{\sigma \in G} \sigma(x)^2$$

belongs to K.

Solution: Part (a) is not correct (by Galois correspondance, $x \in K$ if and only if $\sigma(x) = x$ for all $\sigma \in G$; so $\sigma_0(x) = x$ does not imply $x \in K$ unless σ_0 generates G)

Part (b) is not correct (although G is cyclic, it might be that σ_0 is not a generator)

Part (c) is correct (by Galois correspondance, one checks by reordering the sum that the sum y indicated satisfies $\tau(y) = y$ for all $\tau \in G$, so that $y \in L^G = K$).

7. Let R be a ring and $\mathfrak{a} \subsetneq R$ an ideal. Which of the following statements are true?

(a) For arbitrary $r, s \in R$ we have $r + \mathfrak{a} = s + \mathfrak{a}$ if and only if $r = s$.

(b) If there exists a field K and a ring homomorphism $\varphi : R \to K$, such that $\ker(\varphi) = \mathfrak{a}$, then $\mathfrak{a}$ is a maximal ideal.

(c) We have $(x) + \mathfrak{a} = (1)$ for all $x \in R \backslash \mathfrak{a}$ if and only if $\mathfrak{a}$ is maximal.

(d) If $\mathfrak{a} = (a, b)$ for some elements $a, b \in R$, then $\mathfrak{a}$ is not principal.

Solution: Part (a) is false for $R = \mathbb{Z}$ and $\mathfrak{a} = 2\mathbb{Z}$ since $1 + 2\mathbb{Z} = 3 + 2\mathbb{Z}$, but $1 \neq 3$.

Part (b) is false. For example the canonical injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$ has kernel (0), which is not a maximal ideal of $\mathbb{Z}$. (For a general ring homomorphism $\varphi : R \to K$ the image $\mathrm{im}(\varphi) \simeq R/\ker(\varphi)$ is a subring of K, hence an integral domain, and so $\ker(\varphi)$ is a prime ideal in R, but that is all that one can conclude.)

Part (c) is true: $(\Rightarrow)$: Since $\mathfrak{a}$ is a proper ideal, it is contained in a maximal ideal $\mathfrak{m} \subset R$. If there exists an $x \in \mathfrak{m} \backslash \mathfrak{a}$, then the assumption in (c) implies the existence of an element $a \in \mathfrak{a}$ such that $x + a = 1$. Since $x, a \in \mathfrak{m}$, it follows that $1 \in \mathfrak{m}$ so that $\mathfrak{m} = 1$, a contradiction. Hence $\mathfrak{a} = \mathfrak{m}$.

$(\Leftarrow)$: Let $x \in R \backslash \mathfrak{a}$. Then, since $\mathfrak{a}$ is maximal and $\mathfrak{a} \subsetneq (x) + \mathfrak{a}$, it follows that $(x) + \mathfrak{a} = (1)$.

Part (d) is false: take a or b equal to 1 or 0.

8. Consider the ring $R := \mathbb{Z}[i]$ which, with respect to the norm mapping

$$N : R \to \mathbb{Z}^{>0} : a + bi \mapsto a^2 + b^2$$

is a Euclidean ring. Which of the following statements are correct?

(a) The element 2 is prime in R.

(b) An element $\pi \in R$ is irreducible if and only if $N(\pi)$ is prime.

(c) For any $r_1, \ldots, r_n \in R$ there are elements $x_1, \ldots, x_n \in R$ such that

$$\gcd(r_1, \ldots, r_n) = x_1 r_1 + \ldots + x_n r_n.$$

(d) $\gcd(4 + i, 3 + 5i) \sim 1 - 4i$.

Solution: Part (a) is false. Observe that $2 = (1+i)(1-i)$. We have seen that neither $(1+i)$ nor $(1-i)$ are units in R (see Exercise sheet 1). Therefore 2 is reducible in R. Since prime elements are irreducible, it follows that 2 is not prime.

Part (b) is false. From Exercise sheet 7 we know that primes $p \in \mathbb{Z}$ such that $p \equiv 3(\mathrm{mod}4)$ are prime in R. Since for such p we have $N(p) = p^2$, this provides a counterexample.

Part (c) is true. See course. The statement holds for any principal ideal domain, in particular for Euclidean domains.

Part (d) is true. Direct computation using the euclidean algorithm. We have $4 + i = (3+5i) + (1-4i)$ and $3 + 5i = (-1+i)(1-4i)$.

9. Which of the following polynomials is irreducible?

(a) $\frac{1}{10}X^4 + 3X^3 + 15X + \frac{2}{10}$ in the ring $\mathbb{Q}[X]$.

(b) $X^{2016} + X^{19} + X^2 - 1$ in the ring $\mathbb{Z}/3\mathbb{Z}[X]$.

(c) $Y^3 + (X^2 - 2iX - 1)\,Y^2 + (X^2+1)\,Y - X + i$ in the ring $\mathbb{C}[X, Y]$

Solution: Part (a) is true. Multiply by 10 and use the Eisenstein criterion for $p = 2$.

Part (b) is false. The polynomial has a zero at $X = -1$ and hence the factor $(X + 1)$.

Part (c) is true by the Eisenstein criterion for the prime element $p := X + i$ in $\mathbb{C}[X]$.

10. Consider a ring R, a field K, and a homomorphism $\varphi : R \to K$. Which of the following statements are true?

(a) Then $\ker(\varphi)$ is a prime ideal of R.

(b) If K is finite, R must also be finite.

(c) If R is finite, $\mathrm{im}(\varphi)$ must be a field.

Solution: Part (a) is true. We know that $\mathrm{im}(\varphi)$, being a subring of K, is an integral domain. Since $R/\ker(\varphi) \cong \mathrm{im}(\varphi)$, it follows that $\ker(\varphi)$ is a prime ideal.

Part (b) is false. The canonical projection $\mathbb{F}_p[X] \to \mathbb{F}_p[X]/(X) \cong \mathbb{F}_p$ is a counterexample.

Part (c) is true. We know that $\mathrm{im}(\varphi)$ is a finite integral domain, and each finite integral domain is a field:

Recall that 'cancellation' holds in domains. That is, if $c \neq 0$, then $ac = bc$ implies $a = b$. So, given $x \in \mathrm{im}(\varphi)$, consider $x, x^2, x^3, \ldots$. Since $\mathrm{im}(\varphi)$ is finite, there would be a repetition sometime: $x^n = x^m$ for some integers $n > m$. Then, by cancellation, $x^{n-m} = 1$, and x has an inverse. Hence $\mathrm{im}(\varphi)$ is a field.