**AM 106/206: Applied Algebra** **Prof. Salil Vadhan**

Final Exam Practice Problems

December 2018

**Problem 1. (True/False)** Justify your answers with one or two sentences.

1. There is a field with 6 elements.
2. There is a vector space with 6 elements.
3. There is a group with 6 elements.
4. There is a commutative ring with unity with 6 elements.
5. Every finite group is a subgroup of a permutation group.
6. Every monic polynomial in $\mathbb{F}[x]$, where $\mathbb{F}$ is a field, is the product of monic irreducible polynomials, and this product is unique up to order.
7. The ring $\mathbb{F}[x, y]$ of bivariate polynomial over a field $\mathbb{F}$ is a principal ideal domain.
8. There exists an error-correcting code mapping 20 letter sequences from $\mathbb{Z}_{97}$ to 40 letter sequences over $\mathbb{Z}_{97}$ such that every pair of sequences differ in 20 locations.
9. The multiplicative inverse of an element in the field $\mathbb{F}[x]/\langle p(x)\rangle$ can be computed in poly$(n)$ operations over the field $\mathbb{F}$, where $n = \deg(p)$ a $p(x)$ is a monic irreducible polynomial.
10. If $G$ is a cyclic group of order $n$ and $d|n$, then $G$ contains an element of order $d$.
11. There is a group of order 100 that has a subgroup of order 40.
12. (153) is an even permutation.
13. Groups $\mathbb{Z}_{77}^*$ and $\mathbb{Z}_2 \times \mathbb{Z}_{30}$ are isomorphic.
14. For every prime $p$, there is an integral domain with $p^2$ elements.
15. There is a polynomial-time algorithm that given an integer $N$, finds descriptions of finite fields $F_1$ and $F_2$ such that the ring $\mathbb{Z}_N$ is isomorphic to $F_1 \times F_2$, whenever such fields $F_1$ and $F_2$ exist.
16. $\mathbb{Z}_{91}^*$ is isomorphic to a subgroup of $S_{72}$.
17. For all groups $G, H$ and homomorphisms $\varphi : G \to H$, $G/\ker(varphi) \cong H$.

**Problem 2. (Subgroups of $S_3$)**

1. Draw the subgroup lattice of $S_3$.
2. Find a subgroup $H \leq S_3$ such that the operation of $S_3$ does *not* give a well-defined group operation on the left-cosets of $H$. That is, there are elements $a, a', b, b' \in S_3$ such that $aH = a'H$ and $bH = b'H$, but $abH \neq a'b'H$.
3. For the $H$ you found above, prove that there is no group $G'$ and homomorphism $\varphi : G \to G'$ such that $\ker(\varphi) = H$.

**Problem 3. (Ideals and Factor Rings)**

1. Which elements $a + b\sqrt{2}$ of the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ are contained in the ideal $\langle\sqrt{2}\rangle$?
2. Determine the factor ring $\mathbb{Z}[\sqrt{2}]/\langle\sqrt{2}\rangle$.
3. Is $\langle\sqrt{2}\rangle$ a maximal ideal?

**Problem 4. (Ring Isomorphisms)** For each of the following pairs $(R_1, R_2)$ of rings, determine whether (a) $R_1$ and $R_2$ are isomorphic rings, and (b) the *additive* groups of $R_1$ and $R_2$ are isomorphic.

1. $R_1 = \mathbb{Z}$, $R_2 = \{\text{even integers}\}$ (under ordinary addition and multiplication).
2. $R_1 = \mathbb{Z}_5[x]/\langle x^3 + 2x^2 + x\rangle$, $R_2 = \mathbb{F}_{125}$. (Recall that $\mathbb{F}_{125}$ is the same as GF(125).)
3. $R_1 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, $R_2 = \mathbb{R}[x]/I$ for $I = \{p(x) \in \mathbb{R}[x] : p(1) = p(2) = p(3) = 0\}$.

**Problem 5. (Finite Fields)**

1. List all monic irreducible polynomials of degree 1 in $\mathbb{Z}_3[x]$.
2. Prove that $E = \mathbb{Z}_3[x]/\langle x^3 + 2x^2 + 1\rangle$ is a field.
3. What is the dimension of $E = \mathbb{Z}_3[x]/\langle x^3 + 2x^2 + 1\rangle$ as a vector space over $\mathbb{Z}_3$? What is $|E|$?
4. Let $\alpha$ be a non-zero element of $E$. What are the possible values for $\alpha$'s additive order? What are the possible values for $\alpha$'s multiplicative order?